Guía de instalación y actualización de vCloud Director

vCloud Director 5.1

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/support/pubs.

ES-000749-00



Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

http://www.vmware.com/es/support/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Guía de instalación y actualización del VMware vCloud Director

La *Guía de instalación y actualización del VMware vCloud Director* brinda información en cuanto a la instalación y actualización del software de VMware vCloud Director y la configuración del mismo a fin de que funcione con VMware vCenter™ para ofrecer servicios de VMware vCloud® que estén habilitados para VMware.

Destinatarios

La *Guía de instalación y actualización de VMware vCloud Director* está dirigida a todos aquellos que deseen instalar o actualizar el software de VMware vCloud Director. La información contenida en este manual ha sido preparada para administradores de sistema de experiencia familiarizados con Linux, Windows, redes IP y VMware vSphere®.

Descripción general de la instalación, configuración y actualización de vCloud Director 1

VMware vCloud® combina un grupo de servidores de vCloud Director con la plataforma de vSphere. Para crear un grupo de servidores de vCloud Director, instale el software de vCloud Director en uno o más servidores, conectando los mismos a una base de datos compartida e integre el grupo de servidores de vCloud Director con vSphere.

La configuración inicial de vCloud Director, incluidos los detalles de las conexiones de red y de base de datos, se establece durante la instalación. Al actualizar una instalación existente a una nueva versión de vCloud Director, actualice el software y el esquema de datos de vCloud Director y mantenga las relaciones existentes entre los servidores, la base de datos y vSphere.

Este capítulo cubre los siguientes temas:

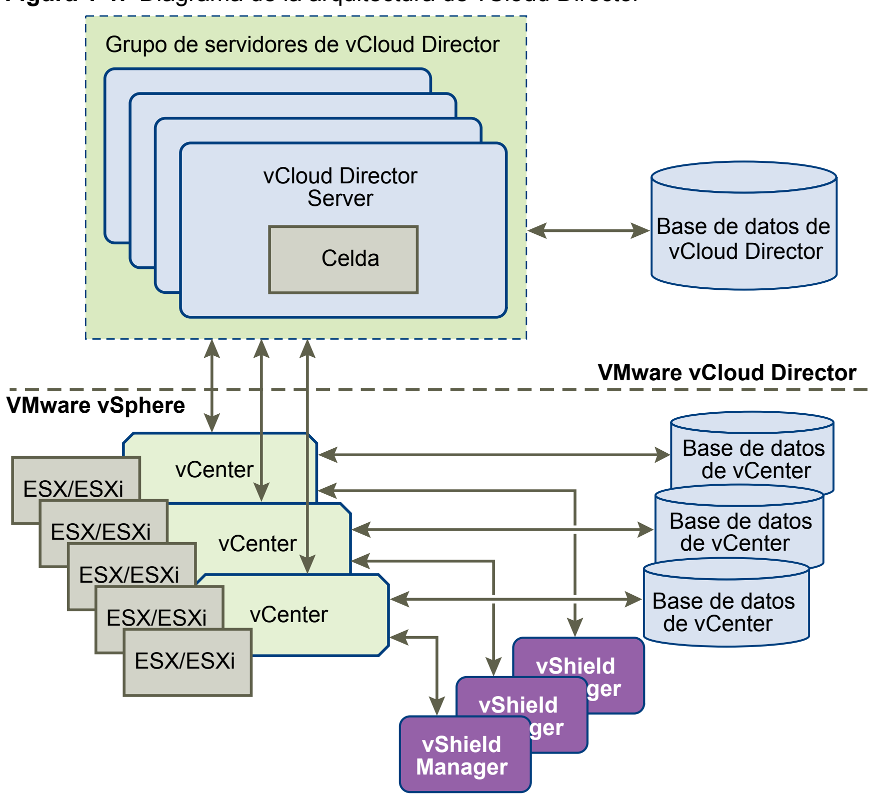
- "Arquitectura de vCloud Director," página 7
- "Planificación de la configuración," página 8
- "Requisitos de hardware y software de vCloud Director," página 9

Arquitectura de vCloud Director

El grupo de servidores de vCloud Director consiste en uno o más vCloud Director Servers. Estos servidores comparten una base de datos común y se vinculan a una cantidad arbitraria de vCenter Servers y hosts ESX/ESXi. Los vShield Manager Servers proporcionan servicios de red a vCenter y a vCloud Director.

La instalación típica crea un grupo de servidores de vCloud Director que comprende varios servidores. Cada servidor del grupo ejecuta una colección de servicios denominada celda de vCloud Director. Todos los miembros del grupo comparten una sola base de datos. Cada celda del grupo se conecta a varios vCenter Servers, los hosts ESX/ESXi que administran y los vShield Manager Servers que se han configurado para ser compatibles con los vCenter Servers.

Figura 1-1. Diagrama de la arquitectura de vCloud Director



El proceso de instalación y configuración de vCloud Director crea las celdas, las conecta a la base de datos compartida y establece las primeras conexiones con un vCenter Server, vShield Manager y hosts ESX/ESXi. A continuación, el administrador del sistema puede utilizar la consola web de vCloud Director para conectar más vCenter Servers, vShield Manager Servers y ESX/ESXi Servers al grupo de servidores de vCloud Director en cualquier momento.

Planificación de la configuración

vSphere proporciona capacidad para almacenamiento, cómputo y redes a vCloud Director. Antes de empezar la instalación, tenga en cuenta la capacidad de vSphere y vCloud Director que necesita, y planee una configuración que pueda dar cabida a la misma.

Los requisitos de configuración dependen de varios factores, incluso la cantidad de organizaciones que haya en la nube, la cantidad de usuarios de cada organización y el nivel de actividad de dichos usuarios. Las directrices siguientes pueden servir como punto de partida para la mayoría de las configuraciones:

- Asigne un vCloud Director Server (celda) por cada vCenter Server que desee poner a disposición en la nube.
- Asegúrese de que todos los vCloud Director Servers cumplan al menos los requisitos mínimos de memoria, CPU y almacenamiento que se especifican en "Requisitos de hardware y software de vCloud Director," página 9.
- Configure la base de datos de vCloud Director como se describe en "Instalación y configuración de una base de datos de vCloud Director," página 14.

Requisitos de hardware y software de vCloud Director

Cada servidor de un grupo de servidores de vCloud Director debe cumplir ciertos requisitos de hardware y de software. Además, debe estar disponible una base de datos accesible para todos los miembros del grupo. Cada grupo de servidores requiere acceso a un vCenter Server, a un vShield Manager Server y a uno o más hosts ESX/ESXi.

Versiones compatibles de vCenter Server, ESX/ESXi y vShield Manager

Existe información actualizada sobre las versiones compatibles de vCenter Server, ESX/ESXi y vShield Manager en *VMware Product Interoperability Matrixes* (Matrices de interoperabilidad de productos VMware) en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Requisitos de configuración de vSphere

Los vCenter Servers y los hosts ESX/ESXi que se pretendan utilizar con vCloud Director deben cumplir requisitos de configuración específicos.

- Las redes de vCenter que se planeen utilizar como redes externas o como grupos de redes de vCloud Director deben estar disponibles para todos los hosts en cualquier clúster destinado para que lo utilice vCloud Director. Al poner dichas redes a disposición de todos los hosts del centro de datos se simplifica la tarea de agregar nuevos vCenter Servers a vCloud Director.
- Debe utilizar switches distribuidos de vSphere para las barreras a través de hosts y para la asignación de grupos de redes.
- Los clústeres de vCenter utilizados con vCloud Director se deben configurar para que utilicen DRS automatizado. DRS automatizado requiere que el almacenamiento compartido esté conectado a todos los hosts de un clúster de DRS.
- Los vCenter Servers deben confiar en los hosts ESX/ESXi. Todos los hosts de todos los clústeres gestionados por vCloud Director deben configurarse para exigir certificados de host verificados. En concreto, debe determinar, comparar y seleccionar huellas digitales coincidentes para todos los hosts. Consulte el apartado Configure SSL Settings incluido en el documento *vCenter Server and Host Management*.

Requisitos de licencia de vSphere

vCloud Director requiere las siguientes licencias de vSphere:

- VMware DRS, licencia otorgada por vSphere Enterprise and Enterprise Plus.
- VMware Distributed Switch y dvFilter, licencia otorgada por vSphere Enterprise Plus. Esta licencia permite crear y utilizar redes aisladas de vCloud Director.

Sistemas operativos compatibles con vCloud Director Server

Tabla 1-1. Sistemas operativos compatibles con vCloud Director Server

Sistema operativo
Red Hat Enterprise Linux 5 (64 bits), Update 4
Red Hat Enterprise Linux 5 (64 bits), Update 5
Red Hat Enterprise Linux 5 (64 bits), Update 6
Red Hat Enterprise Linux 5 (64 bits), Update 8

Tabla 1-1. Sistemas operativos compatibles con vCloud Director Server (Continua)

Sistema operativo
Red Hat Enterprise Linux 6 (64 bits), Update 1
Red Hat Enterprise Linux 6 (64 bits), Update 2

Requisitos de espacio de disco

Cada vCloud Director Server requiere aproximadamente 950 MB de espacio libre para los archivos de instalación y de registro.

Requisitos de memoria

Cada vCloud Director Server debe aprovisionarse con al menos 1 GB de memoria. Se recomiendan 2 GB.

Paquetes de software de Linux

Todos los vCloud Director Servers deben incluir la instalación de varios paquetes de software de Linux. Por lo general, los paquetes se instalan de forma predeterminada con el software del sistema operativo. Si falta alguno, el instalador falla con un mensaje de diagnóstico.

Tabla 1-2. Paquetes de software requeridos

Nombre del paquete	Nombre del paquete	Nombre del paquete
alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	which
krb5-libs	libXt	
libgcc	libXtst	

Bases de datos compatibles con vCloud Director

vCloud Director es compatible con bases de datos Oracle y Microsoft SQL. La información más actualizada sobre las bases de datos compatibles se encuentra disponible en *VMware Product Interoperability Matrixes* (Matrices de interoperabilidad de productos VMware) en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Para obtener las configuraciones de servidor de base de datos recomendadas, véase "Instalación y configuración de una base de datos de vCloud Director," página 14.

Servidores LDAP compatibles

Tabla 1-3. Servidores LDAP compatibles

Plataforma	Servidor LDAP	Métodos de autenticación
Windows Server 2003	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Simple
Windows 7 (2008 R2)	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, Simple SSL

Compatibilidad con SO invitado

Consulte la *Guía de usuario de vCloud Director* para obtener una lista de sistemas operativos invitados compatibles.

Exploradores compatibles con vCloud Director

La consola web de vCloud Director es compatible con varias versiones de los exploradores web Firefox e Internet Explorer.

NOTA: La consola web de vCloud Director es compatible solamente con exploradores de 32 bits. Cuando se indique que un explorador es compatible con una plataforma de 64 bits, se sobreentiende el uso del explorador de 32 bits en la plataforma de 64 bits.

Exploradores admitidos en las plataformas de Microsoft Windows

Tabla 1-4. Compatibilidad con exploradores y sistemas operativos en las plataformas de Microsoft Windows

Plataforma	Internet Explorer 7.*x*	Internet Explorer 8.*x*	Internet Explorer 9.*x*	Firefox 12.*x*, 13.*x*
Windows XP Pro de 32 bits	SÍ	SÍ	No	SÍ
Windows XP Pro de 64 bits	SÍ	SÍ	No	SÍ
Windows Server 2003 Enterprise Edition de 32 bits	SÍ	SÍ	No	SÍ
Windows Server 2003 Enterprise Edition de 64 bits	SÍ	SÍ	No	SÍ
Windows Server 2008	SÍ	SÍ	SÍ	SÍ
Windows Server 2008 R2	No	SÍ	SÍ	SÍ
Windows Vista de 32 bits	SÍ	SÍ	SÍ	SÍ
Windows Vista de 64 bits	SÍ	SÍ	SÍ	SÍ
Windows 7 de 32 bits	No	SÍ	SÍ	SÍ
Windows 7 de 64 bits	No	SÍ	SÍ	SÍ

Exploradores compatibles con las plataformas de Linux

Tabla 1-5. Compatibilidad con exploradores y sistemas operativos en las plataformas de Linux

Plataforma	Firefox 11.*x*
Red Hat Enterprise Linux 5 (32 bits), Update 6	SÍ
Red Hat Enterprise Linux 6 (32 bits)	SÍ
Red Hat Enterprise Linux 6 (64 bits)	SÍ
SLES 11 de 32 bits	SÍ
Ubuntu 10.10 de 32 bits	SÍ
Ubuntu 10.10 de 64 bits	SÍ

Versiones compatibles de Adobe Flash Player

La consola web de vCloud Director requiere Adobe Flash Player versión 10.2 o posterior. Solo se admite la versión de 32 bits.

Versiones de Java admitidas

Los clientes de vCloud Director deben tener la actualización 10 de JRE 1.6.0 o superior instalada y activada. Solo se admite la versión de 32 bits.

Conjuntos de cifrado y versiones compatibles de los protocolos TLS y SSL

vCloud Director requiere que los clientes utilicen SSL. Las versiones admitidas incluyen SSL 3.0 y TLS 1.0. Los conjuntos de cifrado compatibles incluyen los de firma RSA, DSS o de curva elíptica, y los cifrados DES3, AES-128 o AES-256.

Resumen de los requisitos de configuración de red

El funcionamiento seguro y fiable de vCloud Director depende de que la red sea segura y fiable, y que admita la búsqueda directa e inversa de nombres de host, un servicio de temporización de red y otros servicios. La red debe cumplir estos requisitos para poder empezar la instalación de vCloud Director.

La red que conecte los vCloud Director Servers, el servidor de base de datos, los vCenter Servers y los vShield Manager Servers, deben cumplir varios requisitos:

direcciones IP

Cada vCloud Director Server requiere dos direcciones IP para que pueda admitir dos conexiones SSL distintas. Una conexión es para el servicio HTTP. La otra es para el servicio de proxy de consola. Puede utilizar alias de IP o varias interfaces de red para crear dichas direcciones. No puede utilizar el comando `ip addr add` de Linux para crear la segunda dirección.

Dirección del proxy de consola

La dirección IP configurada como dirección del proxy de consola no debe estar ubicada detrás de un equilibrador de cargas que finalice en SSL o de un proxy inverso. Todas las solicitudes de proxy de consola se deben retransmitir directamente a la dirección IP del proxy de consola.

Servicio de temporización de red

Debe utilizar un servicio de temporización de red, tal como NTP, para sincronizar los relojes de todos los vCloud Director Servers, incluso el servidor de base de datos. La diferencia máxima permitida entre los relojes de los servidores sincronizados es de 2 segundos.

Zona horaria de servidor

Todos los servidores de vCloud Director, incluido el servidor de base de datos, deben configurarse dentro de la misma zona horaria.

Resolución de nombre de host

Todos los nombres de host que especifique durante la instalación y configuración de vCloud Director y de vShield Manager deben poder resolverse mediante DNS haciendo uso de búsqueda directa e inversa del nombre de dominio totalmente cualificado o del nombre de host no cualificado. Por ejemplo, para un host de nombre `mycloud.example.com`, ambos comandos siguientes deben ejecutarse correctamente en un host de vCloud Director:

```
nslookup mycloud
nslookup mycloud.example.com
```

Además, si el host `mycloud.example.com` tiene la dirección IP 192.168.1.1, el comando siguiente debe devolver `mycloud.example.com`:

```
nslookup 192.168.1.1
```

Almacenamiento de servidor de transferencia

A fin de proporcionar un almacenamiento temporal para las cargas y las descargas, debe estar accesible un NFS u otro volumen de almacenamiento compartido para todos los servidores del clúster de vCloud Director. Este volumen debe contar con permiso de escritura para el usuario raíz. Cada host debe montar este volumen en `$VCLOUD_HOME/data/transfer`,

habitualmente `/opt/vmware/vcloud-director/data/transfer`. Las cargas y descargas ocupan este almacenamiento desde unas horas hasta un día. Las imágenes transferidas podrían ser grandes, así que asigne al menos varios cientos de gigabytes al volumen.

Recomendaciones para la seguridad de red

El funcionamiento seguro de vCloud Director requiere un entorno de red protegido. Configure y pruebe dicho entorno de red antes de empezar a instalar vCloud Director

Conecte todos los vCloud Director Servers a una red que esté protegida y que se esté supervisando. Las conexiones de red de vCloud Director tienen varios requisitos adicionales:

- No conecte vCloud Director directamente a la red de Internet pública. Siempre proteja las conexiones de red de vCloud Director con un firewall. Solamente el puerto 443 (HTTPS) debe estar abierto para las conexiones entrantes. Los puertos 22 (SSH) y 80 (HTTP) también se pueden abrir para las conexiones entrantes, de ser necesario. El firewall debe rechazar todo el resto del tráfico entrante proveniente de redes públicas.

Tabla 1-6. Puertos que deben permitir paquetes entrantes provenientes de hosts de vCloud Director

Puerto	Protocolo	Comentarios
111	TCP, UDP	Asignador de puertos NFS utilizado por el servicio de transferencia
920	TCP, UDP	rpc.statd de NFS utilizado por el servicio de transferencia
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

No conecte a la red pública los puertos utilizados con las conexiones salientes.

Tabla 1-7. Puertos que deben permitir paquetes salientes provenientes de hosts de vCloud Director

Puerto	Protocolo	Comentarios
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Asignador de puertos NFS utilizado por el servicio de transferencia
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	vCenter, vShield Manager, y conexiones de ESX
514	UDP	Opcional. Permite el uso de syslog
902	TCP	Conexiones de vCenter y de ESX
903	TCP	Conexiones de vCenter y de ESX
920	TCP, UDP	rpc.statd de NFS utilizado por el servicio de transferencia
1433	TCP	Puerto de base de datos de Microsoft SQL Server predeterminado
1521	TCP	Puerto de base de datos Oracle predeterminado
5672	TCP, UDP	Opcional. Mensajes de AMQP para las extensiones de tareas

Tabla 1-7. Puertos que deben permitir paquetes salientes provenientes de hosts de vCloud Director (Continua)

Puerto	Protocolo	Comentarios
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- No conecte los equipos de host físicos a las redes físicas que sean vínculos superiores de los switches distribuidos de vNetwork que respaldan grupos de redes de vCloud Director.
- Tráfico de ruta entre los servidores de vCloud Director y el servidor de base de datos de vCloud Director a través de una red privada dedicada, de ser posible.
- Los switches virtuales y los switches virtuales distribuidos que admitan redes de proveedor deben estar aislados entre ellos. No pueden compartir el mismo segmento de red física de nivel 2.

Instalación y configuración de una base de datos de vCloud Director

Las celdas de vCloud Director utilizan una base de datos para almacenar la información compartida. Dicha base de datos debe existir antes para poder completar la instalación y configuración del software de vCloud Director.

NOTA: Independientemente del software de base de datos que elija, debe crear un esquema de base de datos separado y dedicado para que lo utilice vCloud Director. vCloud Director no puede compartir un esquema de base de datos con ningún otro producto de VMware.

Configuración de una base de datos de Oracle

Las bases de datos de Oracle tienen requisitos de configuración específicos cuando se utilizan con vCloud Director. Instale y configure una instancia de base de datos y cree la cuenta de usuario de la base de datos de vCloud Director antes de instalar vCloud Director.

Procedimiento

1. Configure el servidor de base de datos.

   Un servidor de base de datos configurado con 16 GB de memoria, 100 GB de almacenamiento y 4 CPUs debería ser adecuado para la mayoría de los clústeres de vCloud Director.

2. Cree la instancia de la base de datos.

   Utilice los comandos del formulario siguiente para crear por separado espacios de tabla para datos (CLOUD_DATA) e índice (CLOUD_INDX):

   ```
   Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1000M
   autoextend on;

   Create Tablespace CLOUD_INDX datafile '$ORACLE_HOME/oradata/cloud_indx01.dbf' size 500M
   autoextend on;
   ```

3. Cree la cuenta de usuario de la base de datos de vCloud Director.

   El siguiente comando crea el nombre de usuario de la base de datos `vcloud` con la contraseña `vcloudpass`.

   ```
   Create user $vcloud identified by $vcloudpass default tablespace CLOUD_DATA;
   ```

   NOTA: Al crear la cuenta de usuario de la base de datos de vCloud Director, debe especificar CLOUD_DATA como el espacio de tabla predeterminado.

4 Configure los parámetros de conexión, proceso y transacción de la base de datos.

Debe configurarse la base de datos de modo que permita al menos 75 conexiones por cada celda de vCloud Director, además de alrededor de 50 para el propio uso de Oracle. Puede obtener valores para los demás parámetros de configuración en función de la cantidad de conexiones, donde *C* representa el número de celdas del clúster de vCloud Director.

Parámetro de configuración de Oracle	Valor de las celdas de *C*
CONNECTIONS	75*C+50
PROCESSES	= CONNECTIONS
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

5 Cree la cuenta de usuario de la base de datos de vCloud Director.

No utilice la cuenta del sistema de Oracle como la cuenta de usuario de la base de datos de vCloud Director. Debe crear una cuenta de usuario dedicada para este fin. Conceda los siguientes privilegios del sistema a la cuenta:

- CONNECT
- RESOURCE
- CREATE TRIGGER
- CREATE TYPE
- CREATE VIEW
- CREATE MATERIALIZED VIEW
- CREATE PROCEDURE
- CREATE SEQUENCE

6 Anote el nombre del servicio de la base de datos para que pueda utilizarlo al configurar las conexiones de red y de base de datos.

Para obtener el nombre del servicio de la base de datos, abra el archivo `$ORACLE_HOME/network/admin/tsnames.ora` en el servidor de la base de datos y busque una entrada similar a:

```
(SERVICE_NAME = orcl.example.com)
```

Configuración de una base de datos de Microsoft SQL Server

Las bases de datos de SQL Server tienen requisitos de configuración específicos cuando se utilizan con vCloud Director. Instale y configure una instancia de base de datos y cree la cuenta de usuario de la base de datos de vCloud Director antes de instalar vCloud Director.

El rendimiento de la base de datos de vCloud Director representa un factor importante en el rendimiento y escalabilidad globales de vCloud Director. vCloud Director utiliza el archivo `tmpdb` de SQL Server para almacenar conjuntos grandes de resultados, ordenar o administrar los datos que leen o modifican de manera concurrente. El tamaño de este archivo puede aumentar de manera significativa cuando vCloud Director sufre una fuerte carga concurrente. A modo de buena práctica, se recomienda crear el archivo `tmpdb` en un volumen independiente que tenga un rendimiento rápido de lectura y escritura. Para obtener más información acerca del rendimiento del archivo `tmpdb` y de SQL Server, consulte http://msdn.microsoft.com/en-us/library/ms175527.aspx.

Prerequisitos

- Debe estar familiarizado con el funcionamiento, la creación de scripts y los comandos de Microsoft SQL Server.
- Para configurar Microsoft SQL Server, inicie sesión en el equipo host de SQL Server con las credenciales de administrador. Configure SQL Server para ejecutar la identidad LOCAL_SYSTEM, o cualquier otra identidad con privilegios para ejecutar un servicio de Windows.

Procedimiento

1 Configure el servidor de base de datos.

   Un servidor de base de datos configurado con 16 GB de memoria, 100 GB de almacenamiento y 4 CPUs debería ser adecuado para la mayoría de los clústeres de vCloud Director.

2 Especifique Autenticación en modo mixto durante la configuración de SQL Server.

   No se admite la Autenticación de Windows al utilizar SQL Server con vCloud Director.

3 Cree la instancia de la base de datos.

   El siguiente script crea la base de datos y los archivos de registro, especificando la secuencia de intercalación adecuada.

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

   Los valores que se muestran para SIZE son sugerencias. Puede que tenga que utilizar valores superiores.

4 Establezca el nivel de aislamiento de la transacción.

   El siguiente script establece el nivel de aislamiento de la base de datos en READ_COMMITTED_SNAPSHOT.

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

   Para obtener más información acerca del aislamiento de transacciones, consulte http://msdn.microsoft.com/en-us/library/ms173763.aspx.

5 Cree la cuenta de usuario de la base de datos de vCloud Director.

   El siguiente script crea el nombre de usuario de la base de datos `vcloud` con la contraseña `vcloudpass`.

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

6 Asigne los permisos a la cuenta del usuario de la base de datos de vCloud Director.

El siguiente script asigna la función `db_owner` al usuario de la base de datos creado en Step 5.

```
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

Creación de certificados SSL

vCloud Director requiere SSL para proteger la comunicación entre los clientes y los servidores. Antes de instalar y configurar un grupo de servidores de vCloud Director, debe crear dos certificados para cada miembro del grupo e importar los certificados en los almacenes de claves del host.

Cada vCloud Director Server que planee utilizar en un clúster de vCloud Director requiere dos certificados SSL, uno para cada una de sus direcciones IP.

NOTA: El usuario `vcloud.vcloud` debe poder leer todos los directorios en la ruta a los certificados SSL. El instalador de vCloud Director crea este usuario.

Procedimiento

1 Enumere las direcciones IP del servidor.

Utilice un comando como `ipconfig` para detectar las direcciones IP del servidor.

2 Para cada dirección IP, ejecute el comando siguiente a fin de recuperar el nombre de dominio totalmente cualificado al cual esté enlazada la dirección IP.

`nslookup` *`ip-address`*

3 Anote cada dirección IP, el nombre del dominio totalmente cualificado asociado a ella y si vCloud Director debería utilizar la dirección para el servicio HTTP o para el servicio de proxy de consola.

Necesitará los nombres de dominio totalmente cualificados cuando cree los certificados y las direcciones IP cuando configure las conexiones de red y de base de datos.

4 Cree los certificados.

Puede utilizar certificados firmados por una autoridad de certificación de confianza o bien, certificados de firma automática. Los certificados firmados ofrecen el nivel más alto de confianza. Una longitud de la clave de 2.048 bits proporciona un nivel de seguridad más alto.

Creación e importación de certificados SSL firmados

Los certificados firmados brindan el más alto nivel de confianza en las comunicaciones de SSL.

Cada vCloud Director Server requiere dos certificados SSL, uno por cada una de sus direcciones IP, en el archivo de almacén de claves de Java. Debe crear dos certificados SSL por cada servidor que planee utilizar en el grupo de servidores de vCloud Director. Puede utilizar certificados firmados por una autoridad de certificación de confianza o bien, certificados de firma automática. Los certificados firmados ofrecen el nivel más alto de confianza.

Para crear e importar certificados de firma automática, consulte "Creación de certificados SSL de firma automática," página 20.

Prerequisitos

- Genere una lista de nombres de dominio totalmente cualificados y sus direcciones IP asociadas en este servidor, junto con una opción de servicio para cada dirección IP. Véase "Creación de certificados SSL," página 17.

- Verifique que tenga a acceso al equipo que cuente con Java Runtime Environment versión 6, para que pueda crear el certificado con el comando `keytool`. El instalador de vCloud Director coloca una copia de `keytool` en `/opt/vmware/vcloud-director/jre/bin/keytool`. No obstante, puede realizar este procedimiento en cualquier equipo que tenga instalado Java Runtime Environment versión 6. Los certificados que hayan sido creados con el comando `keytool` desde cualquier otra fuente no se admiten en vCloud Director. El efectuar la creación e importación de los certificados antes de instalar y configurar el software de vCloud Director simplifica el proceso de instalación y configuración. Estos ejemplos de línea de comandos dan por sentado que `keytool` se encuentra en la ruta del usuario. La contraseña del almacén de claves se representa en estos ejemplos como *passwd*.

Procedimiento

1. Cree un certificado que no sea de confianza para el servicio HTTP.

   Este comando crea un certificado que no es de confianza en un archivo de almacén de claves denominado `certificates.ks`.

   ```
   keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -
   alias http
   ```

   El certificado tiene una validez de 90 días.

2. Conteste las preguntas de `keytool`.

   Cuando `keytool` le pida su nombre y apellido, escriba el nombre de dominio totalmente cualificado que esté asociado con la dirección IP que desee utilizar con el servicio HTTP.

3. En las preguntas restantes, proporcione las respuestas correspondientes a su organización y ubicación, tal como se muestra en el ejemplo siguiente.

   ```
   What is your first and last name? [Unknown]:mycloud.example.com
   What is the name of your organizational unit? [Unknown]:Engineering
   What is the name of your organization? [Unknown]:Example Corporation
   What is the name of your City or Locality? [Unknown]:Palo Alto
   What is the name of your State or Province? [Unknown]:California
   What is the two-letter country code for this unit? [Unknown]:US
   Is CN=mycloud.example.com, OU=Engineering, O="Example Corporation", L="Palo Alto",
   ST=California, C=US correct?[no]:yes
   Enter key password for <http> (RETURN if same as keystore password):
   ```

4. Cree una solicitud de firma de certificado para el servicio HTTP.

   Este comando crea una solicitud de firma de certificado en el archivo `http.csr`.

   ```
   keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -certreq -alias http -
   file http.csr
   ```

5. Cree un certificado que no sea de confianza para el servicio proxy de consola.

   Este comando agrega un certificado que no es de confianza al archivo de almacén de datos creado en Step 1.

   ```
   keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -
   alias consoleproxy
   ```

   El certificado tiene una validez de 90 días.

6. Cuando `keytool` le pida su nombre y apellido, escriba el nombre de dominio totalmente cualificado que esté asociado con la dirección IP que desee utilizar con el servicio de proxy de consola.

7. En las preguntas restantes, proporcione las respuestas correspondientes a su organización y ubicación, tal como se muestra en el ejemplo Step 3.

8 Cree una solicitud de firma de certificado para el servicio de proxy de consola.

Este comando crea una solicitud de firma de certificado en el archivo `consoleproxy.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -certreq -alias
consoleproxy -file consoleproxy.csr
```

9 Envíe las solicitudes de firma de certificado a la autoridad de certificación.

Si la autoridad de certificación le exige especificar un tipo de servidor web, utilice Jakarta Tomcat.

10 Cuando reciba los certificados firmados, impórtelos en el archivo de almacén de claves.

a Importe el certificado raíz de la autoridad de certificación en el archivo de almacén de claves.

Este comando importa el certificado raíz del archivo `root.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias root
-file root.cer
```

b (Opcional) Si recibió certificados intermedios, impórtelos en el archivo de almacén de claves.

Este comando importa los certificados intermedios del archivo `intermediate.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias
intermediate -file intermediate.cer
```

c Importe el certificado del servicio HTTP.

Este comando importa el certificado del archivo `http.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias http
-file http.cer
```

d Importe el certificado del servicio de proxy de consola.

Este comando importa el certificado del archivo `consoleproxy.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias
consoleproxy -file consoleproxy.cer
```

11 Para verificar que se hayan importado todos los certificados, vea el contenido del archivo de almacén de claves.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -list
```

12 Repita los pasos del Step 1 al Step 11 en cada vCloud Director Server restante.

Qué hacer a continuación

Si creó el archivo de almacén de claves `certificates.ks` en un equipo que no sea el servidor en el cual haya generado la lista de nombres de dominio totalmente cualificados y sus direcciones IP, copie dicho archivo en ese servidor ahora. Necesita el nombre de la ruta de almacén de claves cuando ejecute el script de configuración. Véase "Configuración de conexiones de red y de base de datos," página 28.

NOTA: Debido a que el script de configuración de vCloud Director no se ejecuta con una identidad privilegiada, cualquier usuario debe poder leer el archivo de almacén de claves y el directorio en el cual se almacene el mismo.

Creación de certificados SSL de firma automática

Los certificados de firma automática ofrecen una manera cómoda de configurar SSL para vCloud Director en entornos donde exista mínima preocupación por la confianza.

Cada vCloud Director Server requiere dos certificados SSL, uno por cada una de sus direcciones IP, en el archivo de almacén de claves de Java. Debe crear dos certificados SSL por cada servidor que planee utilizar en el grupo de servidores de vCloud Director. Puede utilizar certificados firmados por una autoridad de certificación de confianza o bien, certificados de firma automática. Los certificados firmados ofrecen el nivel más alto de confianza.

Para crear e importar certificados firmados, consulte "Creación e importación de certificados SSL firmados," página 17.

Prerequisitos

- Genere una lista de nombres de dominio totalmente cualificados y sus direcciones IP asociadas en este servidor, junto con una opción de servicio para cada dirección IP. Véase "Creación de certificados SSL," página 17.
- Verifique que tenga a acceso al equipo que cuente con Java Runtime Environment versión 6, para que pueda crear el certificado con el comando `keytool`. El instalador de vCloud Director coloca una copia de `keytool` en `/opt/vmware/vcloud-director/jre/bin/keytool`. No obstante, puede realizar este procedimiento en cualquier equipo que tenga instalado Java Runtime Environment versión 6. Los certificados que hayan sido creados con el comando `keytool` desde cualquier otra fuente no se admiten en vCloud Director. El efectuar la creación e importación de los certificados antes de instalar y configurar el software de vCloud Director simplifica el proceso de instalación y configuración. Estos ejemplos de línea de comandos dan por sentado que `keytool` se encuentra en la ruta del usuario. La contraseña del almacén de claves se representa en estos ejemplos como *passwd*.

Procedimiento

1. Cree un certificado que no sea de confianza para el servicio HTTP.

   Este comando crea un certificado que no es de confianza en un archivo de almacén de claves denominado `certificates.ks`.

   ```
   keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -
   alias http
   ```

2. Cree un certificado que no sea de confianza para el servicio proxy de consola.

   Este comando agrega un certificado que no es de confianza al archivo de almacén de datos creado en Step 1.

   ```
   keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -
   alias consoleproxy
   ```

   El certificado tiene una validez de 90 días.

3. Para verificar que se hayan importado todos los certificados, vea el contenido del archivo de almacén de claves.

   ```
   keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -list
   ```

4. Repita de Step 1 a Step 3 en cada vCloud Director Server restante.

Qué hacer a continuación

Si creó el archivo de almacén de claves `certificates.ks` en un equipo que no sea el servidor en el cual haya generado la lista de nombres de dominio totalmente cualificados y sus direcciones IP, copie dicho archivo en ese servidor ahora. Necesita el nombre de la ruta de almacén de claves cuando ejecute el script de configuración. Véase "Configuración de conexiones de red y de base de datos," página 28.

NOTA: Debido a que el script de configuración de vCloud Director no se ejecuta con una identidad privilegiada, cualquier usuario debe poder leer el archivo de almacén de claves y el directorio en el cual se almacene el mismo.

Instalación y configuración de vShield Manager

vCloud Director depende de vShield Manager para ofrecer servicios de red a la nube. Instale y configure vShield Manager antes de empezar a instalar vCloud Director.

Debe asociar cada vCenter Server que agregue a vCloud Director con una instancia única de vShield Manager. Para obtener información en cuanto a los requisitos de red y a las versiones compatibles de vShield Manager, véase "Requisitos de hardware y software de vCloud Director," página 9.

IMPORTANTE: Este procedimiento se aplica solo a las instalaciones nuevas de vCloud Director. Si va a actualizar una instalación existente de vCloud Director, puede actualizar de manera opcional su instalación de vShield Manager asociada. Una versión nueva de vShield Manager no funciona con una versión existente de vCloud Director. Véase "Actualización de vShield Manager," página 50.

Procedimiento

1. Utilice vSphere Client para iniciar sesión en su vCenter Server.
2. Seleccione **Archivo > Implementar plantilla OVF**.
3. Navegue hasta la ubicación donde se encuentre el archivo `vShield Manager.ovf` y siga las indicaciones para implementar el archivo OVF.
4. Una vez que se implemente el archivo OVF, encienda la máquina virtual de vShield Manager y abra la consola.
5. Inicie sesión en la consola con el nombre de usuario **`admin`** y la contraseña **`default`**.
6. En el indicador `manager`, escriba **`enable`**.
7. En el indicador `Password`, escriba **`default`** para habilitar el modo de configuración.

   Una vez que se haya habilitado el modo de configuración, la cadena del indicador cambia a `manager#`.
8. En el indicador `manager#`, escriba **`setup`** para empezar el procedimiento de configuración.
9. Especifique la dirección IP, la máscara de subred y la puerta de enlace predeterminada de la máquina virtual de vShield Manager.

   Esta información es necesaria para adjuntar un vCenter Server a Cloud Director.
10. Escriba **`exit`** para cerrar sesión.
11. Cierre la consola y deje la máquina virtual en ejecución.

    No es necesario que sincronice vShield Manager con vCenter ni que registre vShield Manager como complemento de vSphere Client cuando utilice vShield Manager con vCloud Director.

Instalación y configuración de un broker AMQP

El protocolo de cola de mensajes avanzado (AMQP, Advanced Message Queuing Protocol) es un estándar abierto para poner mensajes en cola que admite mensajes flexibles en sistemas empresariales. vCloud Director incluye un servicio AMQP que se puede configurar para que funcione con un broker AMQP, como RabbitMQ, que ofrece a los operadores de nubes una secuencia de notificaciones de los eventos en la nube. Si desea utilizar este servicio, instale y configure un broker AMQP.

Procedimiento

1. Descargue el servidor de RabbitMQ de http://info.vmware.com/content/12834_rabbitmq.
2. Siga las instrucciones de instalación de RabbitMQ para instalar RabbitMQ en un host apropiado.

   Las celdas de vCloud Director deben poder conectar con el servidor RabbitMQ en la red.
3. Durante la instalación de RabbitMQ, anote los valores que necesitará especificar al configurar vCloud Director para que funcione con esta instalación de RabbitMQ.
   - El nombre de dominio completo del host del servidor RabbitMQ, por ejemplo `amqp.ejemplo.com`.
   - Un nombre de usuario y contraseña válidos para la autenticación con RabbitMQ.
   - El puerto en el que el broker escucha los mensajes. El valor predeterminado es `5672`.
   - El host virtual de RabbitMQ. El valor predeterminado es "`/`".

Qué hacer a continuación

El servicio AMQP de vCloud Director envía mensajes sin cifrar AMQP de manera predeterminada. Si lo configura para cifrar estos mensajes mediante SSL, verifica el certificado del broker utilizando el almacén de confianza JCEKS predeterminado del entorno Java Runtime Environment del servidor de vCloud Director. Java Runtime Environment se encuentra generalmente en el directorio `$JRE_HOME/lib/security/cacerts`.

Para utilizar SSL con el servicio AMQP de vCloud Director, seleccione **Utilizar SSL** en la sección Configuración de broker AMQP de la página Extensibilidad de la consola web de vCloud Director y proporcione:

- un nombre de ruta de certificado SSL o
- un nombre de ruta y contraseña de almacén de confianza de JCEKS

Si no necesita validar el certificado de broker de AMQP, puede seleccionar **Aceptar todos los certificados**.

Descarga e instalación de la clave pública de VMware

El archivo de instalación se firma de manera digital. Para verificar la firma, descargue e instale la clave pública de VMware.

Utilice la herramienta `rpm` de Linux y la clave pública de VMware para verificar la firma digital del archivo de instalación de vCloud Director, o de cualquier otro archivo firmado descargado de `vmware.com`. Si instala la clave pública en el equipo en el que va a instalar vCloud Director, la verificación se realizará como parte de la instalación o actualización. También puede verificar la firma manualmente antes de iniciar la instalación o actualización. En ese caso, utilice el archivo verificado en todas las instalaciones o actualizaciones.

NOTA: El sitio de descarga también publica un valor de suma de comprobación para la descarga. La suma de comprobación se publica de dos formas habituales. La suma de comprobación permite verificar que los contenidos del archivo que ha descargado coinciden con los que se publicaron. No verifica la firma digital.

Procedimiento

1 Obtenga e importe las claves públicas de empaquetado de VMware.

   a Cree un directorio para almacenar las claves públicas de empaquetado de VMware.

   b Utilice un explorador web para descargar todas las claves públicas de empaquetado de VMware desde el directorio http://packages.vmware.com/tools/keys.

   c Guarde los archivos con las claves en el directorio creado.

   d Ejecute el siguiente comando en cada una de las claves que ha descargado para importarlas.

   ```
   # rpm --import /key_path/key_name
   ```

   key_path es el directorio en el que ha guardado las claves.

   key_name es el nombre de archivo de una clave.

2 (Opcional) Utilice la herramienta `rpm` de Linux para verificar la firma digital del archivo descargado.

   ```
   # rpm --checksig installation-file
   ```

   Después de verificar la firma digital del archivo, puede utilizarlo para instalar o actualizar vCloud Director en cualquier servidor, sin tener que instalar la clave pública en dicho servidor. El instalador le avisa si no hay ninguna clave instalada. Ignore la advertencia si ya ha verificado la firma del archivo.

Creación de un grupo de servidores de vCloud Director

2

El grupo de servidores de vCloud Director consiste en uno o más vCloud Director Servers. Cada servidor del grupo ejecuta una colección de servicios denominada celda de vCloud Director. Para crear un grupo de servidores, instale el software de vCloud Director en cada servidor, configure las conexiones de red y base de datos correspondientes, e inicie los servicios de vCloud Director pertinentes.

Requisitos previos para la creación de un grupo de servidores de vCloud Director

IMPORTANTE: Este procedimiento es solo para instalaciones nuevas. Si va a actualizar una instalación existente de vCloud Director, consulte Capítulo 3, "Actualización de vCloud Director," página 35.

Antes de comenzar la instalación y configuración de vCloud Director, realice todas las tareas siguientes.

1. Verifique que esté en funcionamiento un vCenter Server compatible y que el mismo se haya configurado de forma debida para utilizarse con vCloud Director. Para averiguar las versiones compatibles y los requisitos de configuración, véase "Versiones compatibles de vCenter Server, ESX/ESXi y vShield Manager," página 9.
2. Verifique que esté en funcionamiento un vShield Manager Server compatible y que el mismo se haya configurado de forma debida para utilizarse con vCloud Director. Para averiguar las versiones compatibles, véase "Versiones compatibles de vCenter Server, ESX/ESXi y vShield Manager," página 9. Para obtener los detalles de instalación y configuración, véase "Instalación y configuración de vShield Manager," página 21.
3. Verifique que cuente con al menos una plataforma de vCloud Director Server en funcionamiento, la cual se haya configurado con la cantidad debida de memoria y de almacenamiento. Para averiguar las plataformas compatibles y los requisitos de configuración, véase "Sistemas operativos compatibles con vCloud Director Server," página 9.
   - Cada miembro de un grupo de servidores requiere dos direcciones IP: una para admitir una conexión SSL para el servicio HTTP y otra para el servicio de proxy de consola.
   - Cada servidor debe tener un certificado SSL por cada dirección IP. El usuario `vcloud.vcloud` debe poder leer todos los directorios en la ruta a los certificados SSL. El instalador de vCloud Director crea este usuario. Véase "Creación de certificados SSL," página 17.
   - Para el servicio de transferencias, todos los servidores deben montar un NFS o cualquier otro volumen de almacenamiento compartido en `$VCLOUD_HOME/data/transfer`, generalmente `/opt/vmware/vcloud-director/data/transfer`. Este volumen debe contar con permiso de escritura para el usuario raíz.
   - Cada servidor debe tener acceso a un paquete de implementación de Microsoft Sysprep. Véase "Creación de paquetes de implementación de Microsoft Sysprep," página 33.

4 Verifique que se ha creado una base de datos de vCloud Director y que la misma sea accesible para todos los servidores del grupo. Para obtener una lista del software de base de datos compatible, véase "Bases de datos compatibles con vCloud Director," página 10.

- Verifique que ha creado una cuenta para el usuario de a base de datos de vCloud Director y que la cuenta dispone de todos los privilegios de base de datos necesarios. Véase "Instalación y configuración de una base de datos de vCloud Director," página 14.
- Verifique que el servicio de la base de datos se inicie cuando el servidor de base de datos se rearranque.

5 Verifique que todos los vCloud Director Servers, el servidor de la base de datos y todos los vCenter Servers y vShield Manager Servers puedan resolver mutuamente sus nombres, tal como se describe en "Resumen de los requisitos de configuración de red," página 12.

6 Verifique que todos los vCloud Director Servers y el servidor de base de datos estén sincronizados con un servidor horario de la red con las tolerancias mencionadas en "Resumen de los requisitos de configuración de red," página 12.

7 Si planea importar usuarios o grupos a partir de un servicio LDAP, verifique que el servicio sea accesible para cada vCloud Director Server.

8 Abra los puertos de firewall, tal como se ilustra en "Recomendaciones para la seguridad de red," página 13. El puerto 443 debe estar abierto entre los vCloud Director Servers y los vCenter Servers.

Este capítulo cubre los siguientes temas:

Instalación y configuración del software de vCloud Director en cualquier miembro de un grupo de servidores

El instalador de vCloud Director verifica que el servidor de destino cumpla todos los requisitos previos de plataforma e instala el software de vCloud Director en él.

El software de vCloud Director se distribuye como un archivo ejecutable de Linux firmado digitalmente denominado `vmware-vcloud-director-5,1.0-`*nnnnnn*`.bin`, donde *nnnnnn* representa el número de compilación. Después de que se instale el software en el servidor de destino, debe ejecutar un script que configure las conexiones de red y de base de datos del servidor.

Prerequisitos

- Verifique que el servidor de destino y la red que lo conecta cumplan los requisitos especificados en "Resumen de los requisitos de configuración de red," página 12. El servidor de destino no debe tener un usuario o un grupo denominado `vcloud`.
- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Si planea crear un grupo de servidores de vCloud Director que incluya varios servidores, verifique que el servidor de destino monte el almacenamiento de servicio de transferencia compartido en `$VCLOUD_HOME/data/transfer`.

- Si desea que el instalador verifique la firma digital del archivo de instalación, descargue e instale la clave pública de VMware en el servidor de destino. Si ya ha verificado la firma digital del archivo de instalación, no es necesario volver a verificarla durante la instalación. Consulte "Descarga e instalación de la clave pública de VMware," página 22.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Descargue el archivo de instalación en el servidor de destino.

  Si ha comprado el software en un CD o en otro medio, copie el archivo de instalación en una ubicación que sea accesible para todos los servidores de destino.

3 Compruebe que la suma de comprobación de la descarga coincide con la publicada en la página de descargas.

  Los valores de las sumas de comprobación MD5 y SHA1 se publican en la página de descargas. Utilice la herramienta adecuada para verificar que la suma de comprobación del archivo de instalación descargado coincide con el que aparece en la página de descargas. El siguiente comando de Linux valida la suma de comprobación de *archivo-de-instalación* con el valor de *valor-suma-comprobación* MD5 copiado de la página de descargas.

```
md5sum -c checksum-value installation-file
```

4 Asegúrese de que se pueda ejecutar el archivo de instalación.

  El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

```
chmod u+x installation-file
```

5 Ejecute el archivo de instalación en una ventana de consola, shell o terminal.

  Para ejecutar el archivo de instalación, especifique el nombre de ruta completo, por ejemplo `./archivo-de-instalación`. El archivo incluye un script de instalación y un paquete RPM integrado.

  NOTA: No se puede ejecutar el archivo de instalación desde un directorio cuya ruta de acceso incluya espacios integrados.

  El instalador comprueba que el host cumpla todos los requisitos, verifica la firma digital del archivo de instalación, desempaqueta el paquete RPM de vCloud Director e instala el software. El instalador imprime la siguiente advertencia si no ha instalado la clave pública de VMware en el servidor de destino.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

  Después de instalar el software, el instalador le indicará que ejecute el script de configuración, que configura las conexiones de red y base de datos del servidor.

6 Decida en qué momento ejecutar el script de configuración.

Opción	Descripción
Ejecutar el script de configuración ahora	Escriba **y** y pulse Entrar.
Ejecutar el script de configuración posteriormente	Escriba **n** y pulse Entrar para salir del shell.

  Para obtener más información en cuanto a la ejecución del script, véase "Configuración de conexiones de red y de base de datos," página 28.

Configuración de conexiones de red y de base de datos

Después de instalar el software de vCloud Director en el servidor, el instalador le indica que ejecute un script que configura las conexiones de red y de base de datos del servidor.

Debe instalar el software de vCloud Director en el servidor para poder ejecutar el script de configuración. El instalador le indica que ejecute el script después de que se complete la instalación. No obstante, lo puede ejecutar posteriormente. Para ejecutar el script en una operación por separado después de que se instale el software de vCloud Director, inicie sesión como usuario raíz, abra una ventana de consola, shell o terminal, y escriba:

```
/opt/vmware/vcloud-director/bin/configure
```

El script de configuración crea conexiones de red y de base de datos para un solo vCloud Director Server. El script también crea un archivo de respuesta que conserva la información de conexión de la base de datos, la cual se puede utilizar en instalaciones de servidor subsiguientes.

Prerequisitos

- Verifique que una base de datos de un tipo compatible esté accesible desde el vCloud Director Server. Véase "Instalación y configuración de una base de datos de vCloud Director," página 14 y "Requisitos de hardware y software de vCloud Director," página 9.
- Debe tener la siguiente información disponible:
  - Ubicación y contraseña del archivo de almacén de claves que incluya los certificados SSL de este servidor. Véase "Creación e importación de certificados SSL firmados," página 17. El script de configuración no se ejecuta con una identidad privilegiada, de modo que cualquier usuario debe poder leer el archivo de almacén de claves y el directorio en el cual se almacene el mismo.
  - Contraseña de cada certificado SSL.
  - Nombre de host o dirección IP del servidor de base de datos.
  - Nombre y puerto de conexión de la base de datos.
  - Credenciales de usuario de la base de datos (nombre de usuario y contraseña). El usuario debe contar con privilegios de base de datos específicos. Véase "Instalación y configuración de una base de datos de vCloud Director," página 14.

Procedimiento

1 Especifique las direcciones IP que se utilizarán con los servicios de HTTP y de proxy de consola en este host.

   Cada uno de los miembros de un grupo de servidores requiere dos direcciones IP para que pueda admitir dos conexiones SSL distintas: una para el servicio HTTP y otra para el servicio de proxy de consola. Para comenzar el proceso de configuración, elija las direcciones IP detectadas por el script que deben utilizarse con cada servicio.

```
Please indicate which IP address available on this machine should be used
for the HTTP service and which IP address should be used for the remote console proxy.

The HTTP service IP address is used for accessing the user interface and the REST API.
The remote console proxy IP address is used for all remote console (VMRC) connections
and traffic.
Please enter your choice for the HTTP service IP address:
    1: 10.17.118.158
    2: 10.17.118.159
```

```
Choice [default=1]:2
Please enter your choice for the remote console proxy IP address
    1: 10.17.118.158
    Choice [default=1]:
```

2 Especifique la ruta completa al archivo del almacén de claves de Java.

```
Please enter the path to the Java keystore containing your SSL certificates and
private keys:/opt/keystore/certificates.ks
```

3 Especifique las contraseñas del almacén de claves y del certificado.

```
Please enter the password for the keystore:
Please enter the private key password for the 'http' SSL certificate:
Please enter the private key password for the 'consoleproxy' SSL certificate:
```

4 Configure las opciones de administración de mensajes de auditoría.

Los servicios de cada celda de vCloud Director registran los mensajes de auditoría en la base de datos de vCloud Director, donde se conservan por 90 días. Para conservar los mensajes de auditoría durante más tiempo, puede configurar los servicios de vCloud Director para que envíen mensajes de auditoría a la utilidad `syslog` además de a la base de datos de vCloud Director.

Opción	Acción
Para registrar los mensajes de auditoría tanto en `syslog` como en la base de datos de vCloud Director.	Especifique el nombre del host o la dirección IP de `syslog`.
Para registrar los mensajes de auditoría solamente en la base de datos de vCloud Director	Pulse Entrar.

```
If you would like to enable remote audit logging to a syslog
host please enter the hostname or IP address of the syslog server. Audit logs are stored by
vCloud Director for 90 days. Exporting logs via syslog will enable you to
preserve them for as long as necessary.

Syslog host name or IP address [press Enter to skip]:10.150.10.10
```

5 Especifique el puerto en el cual el proceso `syslog` supervisa el servidor especificado.

El puerto predeterminado es 514.

```
What UDP port is the remote syslog server listening on? The
standard syslog port is 514. [default=514]:
Using default value "514" for syslog port.
```

6 Especifique el tipo de base de datos o pulse Entrar para aceptar el valor predeterminado.

```
The following database types are supported:
       1. Oracle
       2. Microsoft SQL Server
Enter the database type [default=1]:
Using default value "1" for database type.
```

7 Especifique la información de conexión de la base de datos.

La información que el script requiere depende del tipo de base de datos que elija. Este ejemplo muestra los indicadores que siguen la especificación de una base de datos de Oracle. Los indicadores de otros tipos de bases de datos son similares.

a Especifique el nombre de host o la dirección IP del servidor de base de datos.

```
Enter the host (or IP address) for the database:10.150.10.78
```

b Especifique el puerto de la base de datos o pulse Entrar para aceptar el valor predeterminado.

```
Enter the database port [default=1521]:
Using default value "1521" for port.
```

c Especifique el nombre del servicio de base de datos.

```
Enter the database service name [default=oracle]:orcl.example.com
```

Si pulsa Entrar, el script de configuración utiliza un valor predeterminado, el cual podría no ser correcto para algunas instalaciones. Si desea obtener información sobre cómo buscar el nombre del servicio de una base de datos de Oracle, véase "Configuración de una base de datos de Oracle," página 14.

d Especifique el nombre de usuario y la contraseña de la base de datos.

```
Enter the database username:vcloud
Enter the database password:
```

El script valida la información que ha proporcionado y luego continúa con otros tres pasos.

1 Inicializa la base de datos y conecta este servidor a la misma.

2 Ofrece el inicio de los servicios de vCloud Director en este host.

3 Muestra una dirección URL en la cual se puede conectar al asistente para la instalación después de que se inicie el servicio de vCloud Director.

Este fragmento muestra una finalización típica del script.

```
Connecting to the database: jdbc:oracle:thin:vcloud/vcloud@10.150.10.78:1521/vcloud
...........
Database configuration complete.
Once the vCloud Director server has been started you will be able to
access the first-time setup wizard at this URL:

    http://vcloud.example.com

Would you like to start the vCloud Director service now? If you choose not
to start it now, you can manually start it at any time using this command:
    service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment).

The service was started; it may be several minutes before it is ready for use.
Please check the logs for complete details.

vCloud Director configuration is now complete. Exiting...
```

Qué hacer a continuación

NOTA: La información de conexión de base de datos y otras respuestas reutilizables que haya proporcionado durante la configuración se conservan en un archivo que se encuentra en `/opt/vmware/vcloud-director/etc/responses.properties` en este servidor. Este archivo contiene información confidencial que debe volver a utilizar al agregar más servidores al grupo de servidores. Conserve el archivo en un lugar seguro y ponerlo a disposición solamente cuando sea necesario.

Para agregar más servidores al grupo, véase "Instalación del software de vCloud Director en servidores adicionales," página 32.

Después de que los servicios de vCloud Director se estén ejecutando en todos los servidores, puede abrir el asistente para la instalación en la dirección URL que se muestra cuando se completa el script. Véase Capítulo 4, "Configuración de vCloud Director," página 55.

Protección y reutilización del archivo de respuesta

Los detalles de conexión de red y de base de datos que proporciona cuando configura la primera instancia del servidor de vCloud Director se guardan en un archivo de respuesta. Este archivo contiene información confidencial que debe volver a utilizar al agregar más servidores al grupo de servidores. Conserve el archivo en un lugar seguro y ponerlo a disposición solamente cuando sea necesario.

El archivo de respuesta se crea en `/opt/vmware/vcloud-director/etc/responses.properties` en el primer servidor para el cual configure las conexiones de red y de base de datos. Cuando agregue más servidores al grupo, debe utilizar una copia del archivo de respuesta para proporcionar los parámetros de configuración que comparten todos los servidores.

Procedimiento

1 Proteja el archivo de respuesta.

   Guarde una copia del archivo en un lugar seguro. Restrinja el acceso al mismo y asegúrese de tener una copia de seguridad en un lugar seguro. Al crear la copia de seguridad del archivo, evite enviar texto no cifrado a través de redes públicas.

2 Vuelva a utilizar el archivo de respuesta.

   Copie el archivo en un lugar donde sea accesible para los servidores que vaya a configurar. El archivo debe ser propiedad de **`vcloud.vcloud`** y el propietario debe tener permiso de lectura y escritura, tal como se muestra en este ejemplo, caso contrario, no se podrá utilizar el script.

   ```
   % ls -l responses.properties
   -rw------- 1 vcloud vcloud 418 Jun 8 13:42
   responses.properties
   ```

Qué hacer a continuación

Tras configurar los servidores adicionales, elimine la copia del archivo de respuesta que utilizó para configurarlos.

Inicio o detención de servicios de vCloud Director

Tras completar la instalación y la configuración de la conexión de base de datos en un servidor, puede iniciar los servicios de vCloud Director en él. También puede detener dichos servicios si se encuentran en ejecución.

El script de configuración le indica que inicie los servicios de vCloud Director. Puede dejar que el script inicie estos servicios, o puede iniciarlos usted mismo más adelante. Los servicios deben estar en ejecución para que pueda finalizar e inicializar la instalación.

Los servicios de vCloud Director se inician siempre que rearranque un servidor.

IMPORTANTE: Si está deteniendo los servicios de vCloud Director como parte de una actualización de software de vCloud Director, deberá utilizar la herramienta de administración de celdas, que le permite poner la celda en modo inactivo antes de detener los servicios. Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 37.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Inicie o detenga los servicios.

Opción	Acción
Iniciar los servicios	Abra una ventana de consola, shell o terminal, y ejecute el comando siguiente. `service vmware-vcd start`
Detenga los servicios cuando se esté utilizando la celda	Utilice la herramienta de administración de celdas.
Detenga los servicios cuando no se esté utilizando la celda	Abra una ventana de consola, shell o terminal, y ejecute el comando siguiente. `service vmware-vcd stop`

Instalación del software de vCloud Director en servidores adicionales

Puede agregar servidores a un grupo de servidores de vCloud Director en cualquier momento. Todos los servidores del grupo de servidores deben configurarse con los mismos detalles de conexión de base de datos. Para asegurarse de que se cumpla este requisito, utilice el archivo de respuesta creado por el procedimiento de instalación del primer servidor a fin de proporcionar dicha información al instalar más servidores.

Prerequisitos

Una copia del archivo de respuesta creado cuando instaló el primer servidor de esta instalación debe estar accesible para cualquier otro servidor que agregue al grupo. Véase "Protección y reutilización del archivo de respuesta," página 31.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Descargue el archivo de instalación en el servidor de destino.

Si ha comprado el software en un CD o en otro medio, copie el archivo de instalación en una ubicación que sea accesible para todos los servidores de destino.

3 Asegúrese de que se pueda ejecutar el archivo de instalación.

El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

```
chmod u+x installation-file
```

4 Ejecute el archivo de instalación, especificando el nombre de la ruta del archivo de respuesta.

Especifique la opción `-r` en la línea de comandos de instalación y especifique el nombre de ruta completo del archivo de respuesta como argumento de la opción.

```
archivo-de-instalación -r ruta-al-archivo-de-respuesta
```

5 (Opcional) Repita este procedimiento con todos los demás servidores que agregue a la instalación.

El instalador solicita información de conexión de red y configura las conexiones de red y de base de datos con las respuestas del archivo de respuesta.

Qué hacer a continuación

Después de que finalice el script de configuración y los servicios de vCloud Director se estén ejecutando en todos los servidores, puede abrir el asistente para la instalación en la dirección URL que se muestra cuando se completa el script. Véase Capítulo 4, “Configuración de vCloud Director,” página 55.

Creación de paquetes de implementación de Microsoft Sysprep

Antes de que vCloud Director pueda realizar una personalización de invitado en máquinas virtuales con ciertos sistemas operativos invitados Windows, debe crear un paquete de implementación Microsoft Sysprep en cada celda de nube en su instalación.

Durante la instalación, vCloud Director coloca algunos archivos en la carpeta `sysprep` en el host de vCloud Director Server. No sobrescriba estos archivos al crear el paquete Sysprep.

Prerequisitos

Acceda a los archivos binarios de Sysprep de Windows 2000, Windows 2003 (32 bits y 64 bits) y Windows XP (32 bits y 64 bits).

Procedimiento

1 Copie los archivos binarios de Sysprep de cada sistema operativo en una ubicación adecuada en el host de vCloud Director Server.

   Cada sistema operativo debe tener su propia carpeta.

   NOTA: Los nombres de carpeta distinguen entre mayúsculas y minúsculas.

SO invitado	Destino de copia
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32 bits)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64 bits)	*SysprepBinariesDirectory* `/win2k3_64`
Windows XP (32 bits)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64 bits)	*SysprepBinariesDirectory* `/winxp_64`

   SysprepBinariesDirectory representa una ubicación donde elija copiar los binarios.

2 Ejecute el comando `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh` *SysprepBinariesDirectory*.

   Por ejemplo, `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles`.

3 Utilice el comando `service vmware-vcd restart` para restablecer la celda de nube.

4 Si tiene varias celdas de nube, copie el paquete y el archivo de propiedades en todas las celdas de nube.

```
scp /opt/vmware/vcloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/vcloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@next_cell_IP:/opt/vmware/vcloud-director/guestcustomization
```

5 Reinicie cada celda de nube donde copie los archivos.

Desinstalación del software de vCloud Director

Utilice el comando `rpm` de Linux para desinstalar el software de vCloud Director de un servidor individual.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Desmonte el almacenamiento de servicio de transferencia que habitualmente se monta en `/opt/vmware/vcloud-director/data/transfer`.

3 Abra una ventana de consola, shell o terminal, y ejecute el comando `rpm`.

```
rpm -e vmware-vcloud-director
```

Actualización de vCloud Director 3

Para actualizar vCloud Director a una nueva versión, instale la nueva versión en cada servidor del grupo de servidores de vCloud Director, actualice la base de datos de vCloud Director y reinicie los servicios de vCloud Director. Debe actualizar también los componentes de vSphere compatibles con vCloud Director, incluidos vShield Manager, vCenter y ESX/ESXi.

Después de actualizar un servidor de vCloud Director, también debe actualizar su base de datos de vCloud Director. La base de datos almacena información en cuanto al estado de tiempo de ejecución del servidor, incluso el estado de todas las tareas de vCloud Director que esté ejecutando. Para asegurarse de que no permanezca ninguna información de tarea no válida en la base de datos después de la actualización, debe asegurarse de que ninguna tarea esté activa en el servidor antes de comenzar la actualización.

IMPORTANTE: El proceso de actualización requiere que actualice vCloud Director, vShield Manager, vCenter y ESX/ESXi. Evite que los usuarios accedan a vCloud Director hasta que haya finalizado la fase de actualización de vShield Manager.

La actualización conserva los artefactos siguientes:

- Los archivos de propiedades locales y globales se copian en la nueva instalación.
- Los archivos de Microsoft Sysprep que se utilizan en la personalización de invitados se copian en la nueva instalación.

Si la nube utiliza un equilibrador de carga, puede actualizar un subconjunto del grupo de servidores mientras mantenga disponibles los servicios existentes en los demás. Si no dispone de un equilibrador de carga, la actualización requiere de tiempo suficiente de inactividad de vCloud Director para actualizar la base de datos en al menos un servidor. También puede actualizar los vCenter Servers registrados si no ejecutan una versión compatible del software de vCenter. La actualización de los vCenter Servers o hosts ESX/ESXi puede aumentar el tiempo de inactividad de vCloud Director, porque no se puede acceder a las máquinas virtuales mientras se estén actualizando los hosts o el vCenter Server.

Actualización de un grupo de servidores de vCloud Director

1 Deshabilite el acceso de los usuarios a vCloud Director. Si lo desea, también puede mostrar un mensaje de mantenimiento mientras se está produciendo la actualización. Consulte "Visualización del mensaje de mantenimiento durante una actualización," página 37.

2 Utilice la herramienta de administración de celdas para poner todas las celdas del grupo de servidores en modo inactivo y apagar los servicios de vCloud Director en cada servidor. Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 37.

3 Actualice el software de vCloud Director en todos los miembros del grupo de servidores. Consulte "Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores," página 45. Puede actualizar los servidores de forma individual o en paralelo, pero no debe reiniciar los servicios de vCloud Director en ningún miembro del grupo actualizado antes de actualizar la base de datos de vCloud Director.

4 Actualice la base de datos de vCloud Director. Consulte "Actualización de la base de datos de vCloud Director," página 48.

5 Reinicie vCloud Director en los servidores actualizados. Consulte "Inicio o detención de servicios de vCloud Director," página 31.

6 Actualice vShield Manager. Todas las instalaciones de vShield Manager registradas en este grupo de servidores deben actualizarse a una versión del software de vShield Manager que sea compatible con la versión de vCloud Director instalada por la actualización. Si el programa de actualización detecta una versión incompatible de vShield Manager, no se permitirá la actualización. Se necesita la versión de vShield Manager más reciente incluida en la lista "Versiones compatibles de vCenter Server, ESX/ESXi y vShield Manager," página 9 para utilizar las funciones de red introducidas en esta versión de vCloud Director. Consulte "Actualización de vShield Manager," página 50

7 Vuelva a habilitar el acceso de los usuarios a vCloud Director.

8 Actualice los hosts ESX/ESXi y de vCenter. Consulte "Actualización de vCenter, hosts ESX/ESXi y dispositivos de vShield Edge," página 50. Todos los vCenter Servers registrados en este grupo de servidores deben actualizarse a una versión del software de vShield Manager que sea compatible con la versión de vCloud Director instalada por la actualización. Una vez completada la actualización de vCloud Director, no se podrá acceder a los vCenter Servers incompatibles. Consulte "Versiones compatibles de vCenter Server, ESX/ESXi y vShield Manager," página 9.

9 Revise los cambios en las redes actualizadas y vuelva a configurar reglas de firewall en caso necesario. Consulte "Cambios en redes actualizadas," página 51.

Uso de un equilibrador de carga para reducir el tiempo de inactividad del servicio

Si utiliza un equilibrador de carga u otra herramienta que pueda forzar las solicitudes para que vayan a servidores específicos, puede actualizar un subconjunto del grupo de servidores mientras mantiene disponibles los servicios en el subconjunto restante. Este método reduce el tiempo de inactividad del servicio de vCloud Director al lapso de tiempo necesario para actualizar la base de datos de vCloud Director.

1 Utilice el equilibrador de carga para redirigir las solicitudes de vCloud Director a un subconjunto de los servidores del grupo. Siga los procedimientos recomendados por el equilibrador de carga.

2 Utilice la herramienta de administración de celdas para poner en modo inactivo las celdas que ya no estén procesando solicitudes y apagar los servicios de vCloud Director en esos servidores. Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 37.

3 Actualice el software de vCloud Director en los miembros del grupo de servidores en los cuales haya detenido vCloud Director, pero no reinicie dichos servicios. Consulte "Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores," página 45.

4 Utilice la herramienta de administración de celdas para poner en modo inactivo las celdas que aún no haya actualizado y apagar los servicios de vCloud Director en esos servidores.

5 Actualice la base de datos de vCloud Director. Consulte "Actualización de la base de datos de vCloud Director," página 48.

6 Reinicie vCloud Director en los servidores actualizados. Consulte "Inicio o detención de servicios de vCloud Director," página 31.

7 Actualice vShield Manager. Consulte "Actualización de vShield Manager," página 50.

8 Actualice los hosts ESX/ESXi y de vCenter. Consulte "Actualización de vCenter, hosts ESX/ESXi y dispositivos de vShield Edge," página 50.

9 Utilice el equilibrador de carga para redirigir las solicitudes de vCloud Director a los servidores actualizados.

10 Actualice el software de vCloud Director en los servidores restantes del grupo y reinicie vCloud Director en dichos servidores a medida se completen las actualizaciones. Consulte "Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores," página 45.

11 Revise los cambios en las redes actualizadas y vuelva a configurar reglas de firewall en caso necesario. Consulte "Cambios en redes actualizadas," página 51.

Visualización del mensaje de mantenimiento durante una actualización

Si espera que el proceso de actualización sea largo y desea que el sistema muestre un mensaje de mantenimiento mientras se realiza la actualización, asegúrese de que se pueda acceder a una celda como mínimo mientras se actualizan las otras. Ejecute el comando `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` en esa celda para activar el mensaje de mantenimiento de celdas.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

Puede ejecutar este comando en una celda antes o después de actualizar esta. Cuando esté listo para actualizar la celda o volver a poner en servicio una celda actualizada, ejecute el siguiente comando en la celda para desactivar el mensaje de mantenimiento.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell stop
```

Este capítulo cubre los siguientes temas:

Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo

Antes de actualizar un vCloud Director Server, utilice la herramienta de administración de celdas para poner en modo inactivo los servicios de vCloud Director y apagarlos en la celda del servidor.

vCloud Director crea un objeto de tarea para controlar y administrar cada operación asincrónica que el usuario solicite. La información en cuanto a todas las tareas que estén en ejecución y las recientemente completadas se almacenan en la base de datos de vCloud Director. Debido a que la actualización de la base de datos invalida esta información de la tarea, cerciórese de que no se esté ejecutando ninguna tarea antes de empezar el proceso de actualización.

Con la herramienta de administración de celdas, puede suspender el programador de tareas a fin de que no se puedan iniciar nuevas tareas, para luego verificar el estado de todas las tareas activas. Puede esperar a que finalicen todas las tareas en ejecución o iniciar sesión en vCloud Director como administrador del sistema y cancelar las mismas. Consulte "Referencia de la herramienta de administración de celdas," página 38. Si no se está ejecutando ninguna tarea, puede utilizar la herramienta de administración de celdas para detener los servicios de vCloud Director.

Prerequisitos

- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Verifique que dispone de credenciales de administrador del sistema de vCloud Director.

Procedimiento

1. Inicie sesión en el servidor de destino como raíz.
2. Utilice la herramienta de administración de celdas para apagar correctamente la celda.
   a. Recupere el estado del trabajo actual.

      El comando `cell-management-tool` proporciona las credenciales del administrador del sistema y devuelve un recuento de los trabajos en ejecución.

      ```
      [root@cell1 /opt/vmware/vcloud-
      director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --status
      Job count = 3
      Is Active = true
      ```

   b. Detenga el programador de tareas para poner la celda en modo inactivo.

      Utilice un comando `cell-management-tool` con el siguiente formato.

      ```
      [root@cell1 /opt/vmware/vcloud-
      director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --quiesce true
      ```

      Este comando evita que se inicien nuevos trabajos. Los trabajos existentes se siguen ejecutando hasta que se finalicen o se cancelen. Para cancelar un trabajo, utilice la consola web de vCloud Director o la API REST.

   c. Cuando el valor de `Job count` es `0` y el de `Is Active` es `false`, es seguro cerrar la celda.

      Utilice un comando `cell-management-tool` con el siguiente formato.

      ```
      [root@cell1 /opt/vmware/vcloud-
      director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --shutdown
      ```

Qué hacer a continuación

Después de que la herramienta de administración de celdas detiene los servicios de vCloud Director en este servidor, puede actualizar el software de vCloud Director del servidor.

Referencia de la herramienta de administración de celdas

La herramienta de administración de celdas es una utilidad de línea de comandos que puede utilizar para gestionar una celda y sus certificados SSL, así como para exportar tablas de la base de datos de vCloud Director. Se necesitan credenciales de superusuario o de administrador del sistema para realizar algunas operaciones.

La herramienta de administración de celdas se instala en `/opt/vmware/vcloud-director/bin/cell-management-tool`.

Lista de comandos disponibles

Para obtener una lista de los comandos de la herramienta de administración de celdas, utilice la siguiente línea de comandos.

```
cell-management-tool -h
```

Ejemplo: Ayuda para la utilización de la herramienta de gestión de celdas

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h

usage: cell-management-tool
 -h,--help             print this message
 -p,--password <arg>   administrator password
 -u,--username <arg>   administrator username

Available commands:
 cell - Manipulates the Cell and core components
 dbextract - Exports the data from the given set of tables
 certificates - Reconfigures the SSL certificates for the cell
 generate-certs - Generates self-signed SSL certificates for use with vCD cell
 recover-password - Change a forgotten System Administrator password. Database credentials are
required

For command specific help:
 cell-management-tool [...] <commandName> -h
```

- Comandos para administrar celdas página 40

  Utilice el comando `cell` de la herramienta de administración de celdas para suspender el programador de tareas a fin de que no se puedan iniciar nuevas tareas, para verificar el estado de las tareas activas y para cerrar la celda correctamente.

- Comandos para exportar tablas de bases de datos página 40

  Utilice el comando `dbextract` de la herramienta de administración de celdas para exportar datos de la base de datos de vCloud Director.

- Comandos para sustituir certificados SSL página 43

  Utilice el comando `certificates` de la herramienta de administración de celdas para sustituir los certificados SSL de la celda.

- Comandos para generar certificados SSL de firma automática página 44

  Utilice el comando `generate-certs` de la herramienta de administración de celdas para generar certificados SSL de firma automática para la celda.

- Recuperación de la contraseña del administrador del sistema página 45

  Si conoce el nombre de usuario y la contraseña de la base de datos de vCloud Director, puede utilizar el comando `recover-password` de la herramienta de administración de celdas para recuperar la contraseña del administrador del sistema de vCloud Director.

Comandos para administrar celdas

Utilice el comando `cell` de la herramienta de administración de celdas para suspender el programador de tareas a fin de que no se puedan iniciar nuevas tareas, para verificar el estado de las tareas activas y para cerrar la celda correctamente.

Para administrar celdas, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell command
```

sysadmin-nombreUsuario	Nombre de usuario de un administrador del sistema de vCloud Director.
sysadmin-contraseña	Contraseña del administrador del sistema de vCloud Director.
comando	Subcomando `cell`.

Tabla 3-1. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cell`

Comando	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--quiesce` (-q)	`true` o `false`	Pone la celda en modo inactivo. El argumento `true` suspende el programador. El argumento `false` reinicia el programador.
`--shutdown` (-s)	Ninguno	Apaga los servicios de vCloud Director en el servidor.
`--status` (-t)	Ninguno	Muestra información en cuanto al número de trabajos que se ejecutan en la celda y el estado de ésta.

Ejemplo: Obtener el estado de una tarea

La línea de comandos `cell-management-tool` proporciona las credenciales del administrador del sistema y devuelve un recuento de los trabajos en ejecución. Cuando el valor de `Job count` es `0` y el de `Is Active` es `false`, puede cerrar la celda de manera segura.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --status
Job count = 3
Is Active = true
```

Comandos para exportar tablas de bases de datos

Utilice el comando `dbextract` de la herramienta de administración de celdas para exportar datos de la base de datos de vCloud Director.

Para exportar tablas de bases de datos, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool dbextract options
```

Tabla 3-2. Opciones y argumentos de la herramienta de administración de celdas, subcomando `dbextract`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`-categories`	Lista separada por comas de categorías de tabla para exportar.	Opcional. `NETWORKING` es la única categoría compatible
`-dataFile`	Ruta absoluta a un archivo que describe los datos para exportar.	Opcional. Si no se suministra, el comando utiliza `$VCLOUD_HOME/etc/data_to_export.properties`. Consulte "Especificación de tablas y columnas para exportar," página 42.
`-dumpFile`	Ruta absoluta a un archivo de volcado.	Todos los datos se exportarán a este archivo.
`-exportSettingsFile`	Ruta absoluta a un archivo de propiedades de configuración de exportación de datos.	Opcional. Si no se suministra, el comando utiliza `$VCLOUD_HOME/etc/data_export_settings.ini`. Consulte "Limitación y ordenación de las filas exportadas," página 42.
`-properties`	Ruta absoluta a un archivo de propiedades de conexión de base de datos.	Opcional. Si no se suministra, el comando utiliza `$VCLOUD_HOME/etc/global.properties`. Consulte "Especificación de un archivo de propiedades," página 41.
`-tables`	Lista separada por comas de tablas.	Opcional. Exporte todas las tablas para ver los nombres de tabla individuales.

Especificación de un archivo de propiedades

De forma predeterminada, el comando `dbextract` extrae datos de la base de datos de vCloud Director utilizando la información de conexión de base de datos incluida en el archivo `$VCLOUD_HOME/etc/global.properties` de la celda actual. Para extraer datos de una base de datos de vCloud Director diferente, especifique las propiedades de conexión de base de datos en un archivo y utilice la opción `-properties` para proporcionar el nombre de ruta a ese archivo en la línea de comandos. El archivo de propiedades es un archivo UTF-8 con el siguiente formato.

```
username=username
password=password
servicename=db_service_name
port=db_connection_port
database-ip=db_server_ip_address
db-type=db_type
```

nombreUsuario	Nombre de usuario de la base de datos de vCloud Director ..
contraseña	Contraseña de la base de datos de vCloud Director ..
nombre_servicio_bd	Nombre del servicio de base de datos. Por ejemplo, `orcl.example.com` .
puerto_conexión_db	Puerto de la base de datos.

dirección_ip_servidor_db	Dirección IP del servidor de base de datos.
tipo_db	Tipo de la base de datos. Debe ser `Oracle` o `MS_SQL` .

Especificación de tablas y columnas para exportar

Para restringir el conjunto de datos exportados, utilice la opción `-exportSettingsFile` para crear un archivo `data_to_export.properties` que especifique tablas individuales y, opcionalmente, columnas para exportar. Es un archivo UTF-8 que contiene cero o más líneas con el formato *NOMBRE_TABLA*:*NOMBRE_COLUMNA*.

NOMBRE_TABLA	Nombre de una tabla de la base de datos. Para ver una lista de nombres de tabla, exporte todas las tablas.
NOMBRE_COLUMNA	El nombre de una columna en el *NOMBRE_TABLA* especificado.

En este ejemplo, el archivo `data_to_export.properties` exporta columnas de las tablas `ACL` y `ADDRESS_TRANSLATION`.

```
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

El comando espera encontrar este archivo en `$VCLOUD_HOME/etc/data_to_export.properties`, pero puede especificar otra ruta si lo desea.

Limitación y ordenación de las filas exportadas

Con cualquier tabla, puede especificar cuántas filas desea exportar y cómo ordenar las filas exportadas. Utilice la opción `-exportSettingsFile` para crear un archivo `data_export_settings.ini` que especifique tablas individuales. Es un archivo UTF-8 que contiene cero o más entradas con el siguiente formato:

```
[TABLE_NAME]
rowlimit=int
orderby=COLUMN_NAME
```

NOMBRE_TABLA	Nombre de una tabla de la base de datos. Para ver una lista de nombres de tabla, exporte todas las tablas.
NOMBRE_COLUMNA	El nombre de una columna en el *NOMBRE_TABLA* especificado.

En este ejemplo el archivo `data_export_settings.ini` limita los datos exportados de la tabla `AUDIT_EVENT` a las primeras 10.000 filas y las ordena según el valor de la columna `event_time`.

```
[AUDIT_EVENT]
rowlimit=100000
orderby=event_time
```

El comando espera encontrar este archivo en `$VCLOUD_HOME/etc/data_export_settings.ini`, pero puede especificar otra ruta si lo desea.

Ejemplo: Exportación de todas las tablas de la base de vCloud Director datos actual.

En este ejemplo se exportan todas las tablas de la base de datos de vCloud Director actual al archivo `/tmp/dbdump` .

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool dbextract -dumpFile /tmp/dbdump
This utility outputs data from your vCloud Director system
that may contain sensitive data.
Do you want to continue and output the data (y/n)?
y
Exporting data now. Please wait for the process to finish
Exported 144 of 145 tables.
```

Comandos para sustituir certificados SSL

Utilice el comando `certificates` de la herramienta de administración de celdas para sustituir los certificados SSL de la celda.

El comando `certificates` de la herramienta de administración de celdas automatiza el proceso de sustituir los certificados existentes de una celda por otros almacenados en el almacén de claves JCEKS. El comando `certificates` le permite sustituir certificados de firma automática por certificados firmados. Para crear un almacén de claves JCEKS que contenga certificados firmados, consulte "Creación e importación de certificados SSL firmados," página 17.

Para sustituir los certificados SSL de una celda, utilice un comando con el siguiente formato:

```
cell-management-tool certificates options
```

Tabla 3-3. Opciones y argumentos de la herramienta de administración de celdas, subcomando `certificates`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--config` (-c)	ruta de acceso completa al archivo `global.properties` de la celda.	De forma predeterminada, es `$VCLOUD_HOME/etc/global.properties`.
`--responses` (-r)	ruta de acceso completa al archivo `responses.properties`	De forma predeterminada, es `$VCLOUD_HOME/etc/responses.properties`.
`--keystore` (-s)	*almacénClaves-nombreRuta*	Nombre de ruta completo al almacén de claves JCEKS que contiene los certificados firmados.
`--keystore-pwd` (-w)	*almacénClaves-contraseña*	Contraseña del almacén de claves JCEKS al que hace referencia la opción `--keystore`.

Ejemplo: Sustitución de certificados

Podrá omitir las opciones `--config` y `--responses`, a menos que esos archivos se hayan movido de sus ubicaciones predeterminadas. En este ejemplo, un almacén de claves en `/tmp/new.ks` tiene la contraseña `kspw`. Este ejemplo sustituye los actuales certificados de la celda por otros incluidos en `/tmp/new.ks`

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool certificates -s /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

NOTA: Tendrá que reiniciar la celda después de sustituir los certificados.

Comandos para generar certificados SSL de firma automática

Utilice el comando `generate-certs` de la herramienta de administración de celdas para generar certificados SSL de firma automática para la celda.

El comando `generate-certs` de la herramienta de administración de celdas automatiza el procedimiento que se muestra en "Creación de certificados SSL de firma automática," página 20.

Para generar certificados SSL de firma automática y añadirlos a un almacén de claves nuevo o existente, utilice una línea de comando con el siguiente formato:

`cell-management-tool generate-certs` *`options`*

Tabla 3-4. Opciones y argumentos de la herramienta de administración de celdas, subcomando `generate-certs`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`-issuer` (-i)	*nombre=valor* [, *nombre=valor*, ...]	Nombre distintivo X.509 del emisor del certificado. De forma predeterminada, es `CN=Unknown`. Si especifica varios pares atributo/valor, sepárelos con comas y escriba el argumento entero entre comillas.
`--out` (-o)	*almacénClaves-nombreRuta*	Nombre de ruta completo al almacén de claves de este host.
`--key-size` (-s)	*clave-tamaño*	Tamaño del par de claves expresado como un número entero de bits. El valor predeterminado es 1024.
`--keystore-pwd` (-w)	*almacénClaves-contraseña*	Contraseña del almacén de claves de este host.
`--expiration` (-x)	*días-hasta-caducidad*	Número de días para que caduquen los certificados. El valor predeterminado es 365.

Ejemplo: Creación de certificados de firma automática

En este ejemplo, tenemos un almacén de claves en `/tmp/cell.ks` con la contraseña `kspw`. Este almacén se va a crear si todavía no existe.

En este ejemplo, los nuevos certificados se crean con los valores predeterminados. El nombre de emisor se establece como `CN=Unknown`. El certificado utiliza cifrado de 1024 bits y caduca un año después de su creación.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool generate-certs -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

En este ejemplo, los nuevos certificados se crean utilizando valores personalizados para el tamaño de clave y el nombre del emisor. El nombre de emisor se establece como `CN=Test, L=London, C=GB`. El certificado utiliza cifrado de 2048 bits y caduca 90 días después de su creación.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool generate-certs -o /tmp/cell.ks -w kspw
 -i "CN=Test, L=London, C=GB" -s 2048 -x 90
New keystore created and written to /tmp/cell.ks.
```

Recuperación de la contraseña del administrador del sistema

Si conoce el nombre de usuario y la contraseña de la base de datos de vCloud Director, puede utilizar el comando `recover-password` de la herramienta de administración de celdas para recuperar la contraseña del administrador del sistema de vCloud Director.

Con el comando `recover-password` de la herramienta de administración de celdas, un usuario que conozca el nombre de usuario y la contraseña de la base de datos de vCloud Director puede recuperar la contraseña del administrador del sistema de vCloud Director.

Para recuperar la contraseña del administrador del sistema, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool recover-password options
```

Tabla 3-5. Opciones y argumentos de la herramienta de administración de celdas, subcomando `recover-password`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--dbuser`	El nombre de usuario de la base de datos de vCloud Director.	Debe proporcionarse en la línea de comandos.
`--dbpassword`	Contraseña del usuario de la base de datos de vCloud Director.	Si no se proporciona, se mostrará un indicador solicitando que se introduzca uno.

Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores

El instalador de vCloud Director verifica que el servidor de destino cumpla todos los requisitos previos de la actualización y actualiza el software de vCloud Director en el servidor.

El software de vCloud Director se distribuye como archivo ejecutable de Linux denominado `vmware-vcloud-director-5,1.0-`*nnnnnn*`.bin`, donde *nnnnnn* representa el número de compilación. Después de que se instale la actualización en un miembro del grupo de servidores, debe ejecutar una herramienta que actualiza la base de datos de vCloud Director que el grupo utiliza antes de poder reiniciar los servicios de vCloud Director en el servidor actualizado.

Prerequisitos

- Compruebe que todas las organizaciones del sistema que contienen una red de organización incluyen también un vDC de organización. Dado que el proceso de actualización convierte las redes de organización existentes en redes de vDCs de organización, las organizaciones que contienen redes de organización, pero no incluyen un vDC de organización no podrán actualizarse y fallará la actualización de la base de datos.
- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Si desea que el instalador verifique la firma digital del archivo de instalación, descargue e instale la clave pública de VMware en el servidor de destino. Si ya ha verificado la firma digital del archivo de instalación, no es necesario volver a verificarla durante la instalación. Consulte "Descarga e instalación de la clave pública de VMware," página 22.
- Utilice la herramienta de administración de celdas para poner en modo inactivo y apagar los servicios de vCloud Director en la celda del servidor.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Descargue el archivo de instalación en el servidor de destino.

Si ha comprado el software en un CD o en otro medio, copie el archivo de instalación en una ubicación que sea accesible para todos los servidores de destino.

3 Compruebe que la suma de comprobación de la descarga coincide con la publicada en la página de descargas.

Los valores de las sumas de comprobación MD5 y SHA1 se publican en la página de descargas. Utilice la herramienta adecuada para verificar que la suma de comprobación del archivo de instalación descargado coincide con el que aparece en la página de descargas. El siguiente comando de Linux valida la suma de comprobación de *archivo-de-instalación* con el valor de *valor-suma-comprobación* MD5 copiado de la página de descargas.

```
md5sum -c checksum-value installation-file
```

4 Asegúrese de que se pueda ejecutar el archivo de instalación.

El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

```
chmod u+x installation-file
```

5 Utilice la herramienta de administración de celdas para poner en modo inactivo la celda y apagar los servicios de vCloud Director en el servidor.

Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 37.

6 Ejecute el archivo de instalación en una ventana de consola, shell o terminal.

Para ejecutar el archivo de instalación, especifique el nombre de ruta completo, por ejemplo `./archivo-de-instalación`. El archivo incluye un script de instalación y un paquete RPM integrado.

NOTA: No se puede ejecutar el archivo de instalación desde un directorio cuya ruta de acceso incluya espacios integrados.

Si el instalador detecta una versión de vCloud Director instalada en este servidor que sea igual o posterior que la versión del archivo de instalación, muestra un mensaje de error y sale. Caso contrario, le pide que confirme que está listo para actualizar el servidor.

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
An older version of VMware vCloud Director has been detected.  Would you like
to upgrade it?  The installer will stop the vmware-vcd service,
back up any configuration files from the previous release and migrate the
product configuration as necessary.
```

7 Responda al indicador de actualización.

Opción	Acción
Continuar la actualización.	Escriba **y**.
Salir del shell sin realizar ningún cambio en la instalación actual.	Escriba **n**.

Tras confirmar que está listo para actualizar el servidor, el instalador verifica que el host cumpla todos los requisitos, desempaca el paquete RPM de vCloud Director, detiene los servicios de vCloud Director en el servidor y actualiza el software de vCloud Director que esté instalado.

```
Would you like to upgrade now? (y/n) y
Extracting vmware-vcloud-director ......done
Upgrading VMware vCloud Director...
Installing the VMware vCloud Director
Preparing...                ##################################################
vmware-vcloud-director      ##################################################
Migrating settings and files from previous release...done
Migrating in-progress file transfers to /opt/vmware/vcloud-director/data/transfer...done
Uninstalling previous release...done
```

El instalador imprime la siguiente advertencia si no ha instalado la clave pública de VMware en el servidor de destino.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

8 (Opcional) Actualice las propiedades de registro.

Después de una actualización, las nuevas propiedades de registro se escriben en el archivo `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Opción	Acción
Si no ha cambiado las propiedades de registro existentes	Copie este archivo en `/opt/vmware/vcloud-director/etc/log4j.properties`.
Si ha cambiado las propiedades de registro	Combine el archivo `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` con el archivo `/opt/vmware/vcloud-director/etc/log4j.properties` existente. Al combinar estos archivos se mantienen los cambios.

Una vez que finaliza la actualización del software de vCloud Director, el instalador muestra un mensaje que indica dónde están almacenados los archivos de configuración anteriores y luego le recuerda que ejecute la herramienta de actualización de la base de datos.

Qué hacer a continuación

- Si aún no lo ha hecho, actualice la base de datos de vCloud Director que este servidor utiliza.

- Si ya actualizó la base de datos de vCloud Director que utiliza este grupo de servidores, puede reiniciar el servidor actualizado. Véase "Inicio o detención de servicios de vCloud Director," página 31.

Actualización de la base de datos de vCloud Director

Después de actualizar un servidor en el grupo de servidores de vCloud Director, debe actualizar la base de datos de vCloud Director del grupo para poder reiniciar los servicios de vCloud Director en el servidor.

Todos los servidores de un grupo de servidores de vCloud Director comparten la misma base de datos; por eso, independientemente del grupo que servidores que vaya a actualizar, solo tendrá que actualizar la base de datos una vez. Una vez actualizada la base de datos, los vCloud Director Servers no se podrán conectar a ella hasta que no se hayan actualizado también.

Prerequisitos

IMPORTANTE: Cree una copia de seguridad de la base de datos existente antes de actualizarla. Utilice los procedimientos que el proveedor del software de base de datos recomienda.

- Verifique que ningún vCloud Director Server esté utilizando la base de datos. Véase "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 37

Procedimiento

1 Abra una ventana de consola, shell o terminal, y escriba el comando siguiente para ejecutar el script de actualización de base de datos.

```
/opt/vmware/vcloud-director/bin/upgrade
```

IMPORTANTE: Si el script de actualización de base de datos detecta que se ha registrado una versión incompatible de vShield Manager en esta instalación de vCloud Director, muestra este mensaje de aviso y cancela la actualización.

```
One or more vShield Manager servers registered to this vCloud
Director installation are not supported by the version of vCloud Director
you are upgrading to. Upgrade canceled, please follow the procedures in
the vShield Manager Upgrade Guide to upgrade those unsupported vShield
Manager servers to vShield Manager version 5.0 or later versions.
```

Consulte "Actualización de vShield Manager," página 50.

2 Responda al indicador de actualización de base de datos.

```
Welcome to the vCloud Director upgrade utility

This utility will apply several updates to the database. Please
ensure you have created a backup of your database prior to continuing.

Do you wish to upgrade the product now? [Y/N]: y
```

Opción	Acción
Continuar la actualización.	Escriba **y**.
Salir del shell sin realizar ningún cambio en la base de datos de vCloud Director actual.	Escriba **n**.

La herramienta de actualización de base de datos se ejecuta y muestra mensajes del progreso.

```
Examining database at URL: jdbc:oracle:thin:@10.26.50.54:1521/orcl
Applying 1 upgrade batches
Executing upgrade batch:
Executing SQL statements from file: cc-tool-uninstall-graceful.sql
.....................................
Executing SQL statements from file: Upgrade.sql []
.....................................
Executing SQL statements from file: Upgrade_Data.sql []
.....................................
Executing SQL statements from file: NewInstall_Indexes.sql []
.....................................
Executing SQL statements from file: Upgrade_UUID.sql []
.....................................
Executing SQL statements from file: NewInstall_Funcs.sql []
.....................................

Successfully applied upgrade batch:
Running 2 upgrade tasks
Successfully ran upgrade task
Successfully ran upgrade task
Applying 1 upgrade batches
Executing upgrade batch: cleanup
Executing SQL statements from file: NewInstall_Funcs.sql []
.....................................
Executing SQL statements from file: Upgrade_UUID_Clean.sql []
.....................................
Executing SQL statements from file: Upgrade_Clean.sql []
.....................................

Successfully applied upgrade batch: cleanup
Database upgrade complete
++++++++++++++++++++++++++++++++
```

3 (Opcional) Vuelva a crear los índices de base de datos y actualice las estadísticas de base de datos.

   Estos pasos son opciones y pueden conducir a un mejor rendimiento de la base de datos tras la actualización.

```
Do you wish to rebuild the database indexes? This may take several minutes. [Y/N] y
Rebuilding database indexes

...
Do you wish to update the database statistics? This may take several minutes. [Y/N] y
Updating database statistics
...
```

Una vez actualizada la base de datos, el script de actualización ofrecerá iniciar los servicios de vCloud Director en este host.

```
Would you like to start the vCloud Director service now? If you choose not
to start it now, you can manually start it at any time using this command:
    service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment).
```

Actualización de vShield Manager

Para poder actualizar los hosts de vCenter y ESX/ESXi registrados en vCloud Director, debe actualizar los servidores de vShield Manager asociados a los vCenter Servers.

Para poder actualizar un vCenter Server asociado a vCloud Director, actualice el servidor de vShield Manager asociado al vCenter Server actualizado. Al actualizar vShield Manager se interrumpe el acceso a las funciones administrativas de vShield Manager, aunque esto no afecta a los servicios de red.

Prerequisitos

Debe haber al menos una celda actualizada en ejecución en la instalación de vCloud Director para poder iniciar esta actualización. La celda es la responsable de escribir los datos sobre el vShield Manager actualizado en la base de datos de vCloud Director.

Procedimiento

1 Actualice vShield Manager.

   Siga el procedimiento en la *Guía de inicio rápido de vShield*. Una vez completada la actualización, vShield Manager informa a vCloud Director de que tiene una versión nueva. Pueden pasar varios minutos hasta que vShield Manager envíe la notificación y vCloud Director la procese.

2 Después de actualizar vShield Manager, deberá actualizar todos los hosts de vCenter y ESX/ESXi para poder actualizar los dispositivos de vShield Edge que gestiona el vShield Manager actualizado.

Actualización de vCenter, hosts ESX/ESXi y dispositivos de vShield Edge

Después de haber actualizado vCloud Director y vShield Manager, actualice los vCenter Servers y los hosts ESX/ESXi adjuntos a la nube y, a continuación, actualice los dispositivos de vShield Edge en vCenter Servers actualizados.

Procedimiento

1 Actualice el vCenter Server.

   Consulte la *Guía de instalación y configuración de vSphere*.

2 Actualice el registro del vCenter Server con vCloud Director.

   a En la consola web de vCloud Director, haga clic en la pestaña **Administrar y supervisar** y haga clic en **vCenters** en el panel izquierdo.

   b Haga clic con el botón secundario en el nombre de vCenter Server y seleccione **Actualizar**.

   c Haga clic en **Sí**.

3 Actualice los hosts ESX/ESXi que admite el vCenter Server actualizado.

   Consulte la *Guía de instalación y configuración de vSphere*. Con cada host, la actualización requiere los siguientes pasos:

   a En la consola web de vCloud Director, deshabilite el host.

      En la página **Gestionar y Supervisar**, haga clic en **Hosts** y, a continuación, haga clic con el botón secundario y seleccione **Deshabilitar host**.

   b Utilice vCenter para poner el host en modo de mantenimiento y permitir que todas las máquinas virtuales de dicho host se migren a otro host.

c Actualice el host.

Para garantizar que tiene suficiente capacidad de host actualizado para dar soporte a las máquinas virtuales de su nube, actualice los hosts en lotes pequeños. Cuando realice este paso, las actualizaciones de los agentes de host se completarán a tiempo para permitir que las máquinas virtuales vuelvan a migrar al host actualizado.

d Utilice vCenter para volver a conectar el host.

e Actualice el agente de host de vCloud Director en el host.

Consulte el apartado "Actualizar un agente de host ESX/ESXi" en la *Guía del administrador de vCloud Director*.

f En la consola web de vCloud Director, habilite el host.

En la página **Gestionar y Supervisar**, haga clic en **Hosts** y, a continuación, haga clic con el botón secundario y seleccione **Habilitar host**.

g Utilice vCenter para finalizar el modo de mantenimiento del host.

4 Actualice todos los dispositivos de vShield Edge gestionados por vShield Manager en el vCenter Server actualizado.

Utilice la interfaz de usuario de vShield Manager para administrar esta actualización.

NOTA: Si utiliza la consola web de vCloud Director o la API REST para restablecer una red protegida por vShield Edge, esta actualización se produce de manera automática. Al utilizar la interfaz de usuario de vShield Manager para administrar vShield Edge se obtiene un mejor control administrativo sobre el proceso de actualización y el tiempo de inactividad de la red correspondiente.

Cambios en redes actualizadas

Debido a los cambios en la infraestructura de redes de vCloud Director, en algunas ocasiones las redes y servicios existentes se ven modificados por el proceso de actualización. Si bien ninguna de estas modificaciones afecta a las conexiones de red, es posible que sea necesaria una reconfiguración posterior a la actualización de algunos servicios de red.

Redes de organización

Cuando se actualiza vCloud Director a esta versión, las redes de organización existentes se convierten para utilizar la nueva infraestructura de redes de vCloud Director. Los cambios que es probable que se produzcan en las redes de organización actualizadas son:

- Las redes de organización con enrutamiento se convierten en redes de vDC de organización. Estas redes se conectan a una puerta de enlace Edge de uno de sus vDCs de organización. Los servicios, como NAT y firewall, que se habían definido en la red de organización, se definen ahora en la puerta de enlace Edge. Si su organización tiene varios vDCs, las redes de vDC de organización creadas durante una actualización se comparten en todos los vDCs de la organización.
- Las redes de organización aisladas se convierten en redes de vDC de organización aisladas.
- Las redes de organización conectadas directamente permanecen invariables.
- Las redes de un nuevo vDC de organización utilizan el grupo de redes asignado al vDC de organización en el que se crea la red.
- Las reglas NAT de redes de organización con enrutamiento se convierten en reglas NAT de puerta de enlace Edge. El efecto de cada regla permanece igual aunque la regla se expresa de otra manera. Consulte la *Guía del administrador de vCloud Director* para obtener más información sobre las reglas NAT. Las reglas NAT de las redes de vApps permanecen invariables.

Puertas de enlace Edge y redes de vApps

Los servicios y reglas de firewall se han modificado para permitir una configuración más flexible de las puertas de enlace Edge y las redes de vApps.

Después de una actualización, todos los servicios de firewall de las puertas de enlace Edge y redes de vApps con enrutamiento se ejecutan en modo de compatibilidad, el cual conserva la semántica operativa de sus reglas de firewall. Después de convertir las reglas de firewall existentes al formato actual, puede actualizar las redes para eliminar las limitaciones impuestas por el modo de compatibilidad. Consulte la *Guía del administrador de vCloud Director* para obtener más información sobre las reglas de firewall.

Limitaciones de red en el modo de compatibilidad

Cuando el sistema se encuentra en el modo de compatibilidad, existen varias limitaciones.

- Cada puerta de enlace Edge admite un único vínculo superior y una única interfaz interna; por lo tanto, solo podrá haber una red de vDC de organización con enrutamiento por cada puerta de enlace Edge.
- Las reglas de firewall de la versión 5.1 no se pueden crear en un servicio de firewall.

Para eliminar estas limitaciones, consulte "Reconfiguración de puertas de enlace Edge y redes de vApps para habilitar el funcionamiento normal," página 52

Reconfiguración de puertas de enlace Edge y redes de vApps para habilitar el funcionamiento normal

Después de convertir las reglas de firewall existentes al formato actual, puede volver a configurar las puertas de enlace Edge y las redes de vApps para habilitar el funcionamiento normal y eliminar las limitaciones impuestas por el modo de compatibilidad.

En las versiones anteriores de vCloud Director, las reglas de firewall especificaban la dirección de los paquetes sujetos a la regla. A partir de esta versión, la dirección del paquete se deriva de las direcciones IP de origen y de destino. En la dirección IP **Origen** o **Destino** de una regla de firewall, ahora puede utilizar las palabras clave `interna` y `externa`, además de la palabra clave `cualquiera` o una dirección IP.

Después de una actualización, todos los servicios de firewall de las puertas de enlace Edge y redes de vApps se ejecutan en modo de compatibilidad, el cual conserva la semántica operativa de sus reglas de firewall. Después de convertir las reglas de firewall existentes al formato actual, puede actualizar las redes para eliminar las limitaciones impuestas por el modo de compatibilidad. Consulte la *Guía del administrador de vCloud Director* para obtener más información sobre las reglas de firewall.

Procedimiento

1 Vuelva a implementar todas las puertas de enlace Edge.

   Haga clic con el botón secundario en cada puerta de enlace Edge y seleccione **Volver a implementar**.

2 Vuelva a implementar todas las redes de vApps.

   Haga clic con el botón secundario en cada red de vApp y seleccione **Restablecer red**.

3 Convierta todas las reglas de firewall de puerta de enlace Edge al formato actual.

   Puede hacer clic en **Convertir reglas** en la pestaña **Firewall** de la página **Servicios de puerta de enlace Edge** para convertir automáticamente las reglas. También puede convertir las reglas de forma manual.

   a En la pestaña **Firewall** de la página **Servicios de puerta de enlace Edge**, seleccione la regla y haga clic en **Editar**.

   b Deje sin marcar la casilla **Emparejar regla en IP traducida**.

c Siempre que se utilice `cualquiera` para especificar una dirección IP **Origen** o **Destino**, utilice `interna` o `externa` en su lugar.

d Si la regla está pensada para proporcionar la NAT de destino, cambie la dirección IP **Destino** de `interna` a `externa`.

4 Convierta todas las reglas de firewall de red de vApp al formato actual.

Puede hacer clic en **Convertir reglas** en la pestaña **Firewall** de la página **Configurar servicios** para convertir automáticamente las reglas. También puede convertir las reglas de forma manual.

a En la pestaña **Firewall** de la página **Configurar servicios** de una red de vApp, seleccione la regla y haga clic en **Editar**.

b Deje sin marcar la casilla **Emparejar regla en IP traducida**.

c Siempre que se utilice `cualquiera` para especificar una dirección IP **Origen** o **Destino**, utilice `interna` o `externa` en su lugar.

d Si la regla está pensada para proporcionar la NAT de destino, cambie la dirección IP **Destino** de `interna` a `externa`.

5 Vuelva a configurar todas las puertas de enlace Edge para eliminar las limitaciones del modo de compatibilidad.

En la pestaña **General** de la página Propiedades de puerta de enlace Edge, seleccione **Habilitar compatibilidad con múltiples interfaces**.

6 Vuelva a configurar todas las redes de vApps para eliminar las limitaciones del modo de compatibilidad.

a Haga clic en la pestaña **Mi nube** y haga clic en **vApp** en el panel izquierdo.

b Haga clic con el botón secundario del ratón en una vApp y seleccione **Abrir**.

c En la pestaña **Redes**, active **Mostrar detalles de redes**.

d Haga clic con el botón secundario en la red de vApp y seleccione **Configurar servicios**.

e En la pestaña **Firewall**, seleccione **Emparejar reglas en direcciones originales únicamente**.

Configuración de vCloud Director 4

Después de configurar todos los servidores del grupo de servidores de vCloud Director y de conectarlos a la base de datos, puede inicializar la base de datos del grupo de servidores con una clave de licencia, una cuenta de administrador del sistema y la información asociada. Una vez que finalice este proceso, puede utilizar la consola web de vCloud Director para completar el aprovisionamiento de la nube.

Para poder ejecutar la consola web de vCloud Director, debe ejecutar el asistente para configuración, el cual recopila la información que la consola web requiere para poder iniciarse. Después de que finalice el asistente, la consola web se inicia y muestra la pantalla de inicio de sesión. La consola web de vCloud Director proporciona un conjunto de herramientas para el aprovisionamiento y la administración de nubes. Incluye una función de inicio rápido que le guía por pasos, como la forma de adjuntar vCloud Director a vCenter y de crear una organización.

Prerequisitos

- Complete la instalación de todos los vCloud Director Servers y verifique que los servicios de vCloud Director se hayan iniciado en todos los servidores.
- Verifique que tenga la dirección URL que el script de configuración muestra cuando finaliza.

NOTA: Para averiguar la dirección URL del asistente para configuración después de que salga el script, busque el nombre de dominio totalmente cualificado con la dirección IP que especificó para el servicio HTTP durante la instalación del primer servidor y utilícelo para construir una dirección URL con el formato https://*nombre-de-dominio-totalmente-cualificado*, por ejemplo, https://minube.ejemplo.com. Puede conectarse con el asistente en esa dirección URL.

Complete la instalación de todos los vCloud Director Servers y verifique que los servicios de vCloud Director se hayan iniciado en todos los servidores.

Procedimiento

1 Abra un explorador web y conéctese a la dirección URL que el script de configuración muestra cuando finaliza.

2 Siga las indicaciones para completar la configuración.

Este capítulo cubre los siguientes temas:

Lectura del contrato de licencia

Para poder configurar un grupo de servidores de vCloud Director debe leer y aceptar el contrato de licencia de usuario final.

Procedimiento

1 Lea el contrato de licencia.

2 Acepte o rechace el contrato.

Opción	Acción
Para aceptar el contrato de licencia.	Haga clic en **Sí, acepto los términos del contrato de licencia**.
Para rechazar el contrato de licencia.	**No, no acepto los términos del contrato de licencia**.

Si rechaza el contrato de licencia, no puede continuar con la configuración de vCloud Director.

Especificación de la clave de licencia

Cada clúster de vCloud Director requiere una licencia para su ejecución. La licencia se especifica a modo de número de serie de producto. El número de serie de producto se almacena en la base de datos de vCloud Director.

El número de serie de producto de vCloud Director no es el mismo que la clave de licencia del vCenter Server. Para utilizar vCloud, debe disponer de un número de serie de producto de vCloud Director y de una clave de licencia de vCenter Server. Puede obtener ambos tipos de claves de licencia en el Portal de licencias de VMware.

Procedimiento

1 Obtenga un número de serie de producto de vCloud Director en el Portal de licencias de VMware.

2 Especifique el número de serie de producto en el cuadro de texto **Número de serie del producto**.

Creación de una cuenta de administrador del sistema

Especifique el nombre de usuario, la contraseña y la información de contacto del administrador del sistema de vCloud Director.

El administrador del sistema de vCloud Director tiene privilegios de superusuario en toda la nube. La cuenta inicial de administrador del sistema se crea durante la instalación de vCloud Director. Tras completar la instalación y configuración, el administrador del sistema puede crear otras cuentas de administrador como sea necesario.

Procedimiento

1 Especifique el nombre de usuario del administrador del sistema.

2 Especifique la contraseña del administrador del sistema y confírmela.

3 Especifique el nombre completo del administrador del sistema.

4 Especifique la dirección de correo electrónico del administrador del sistema.

Especificación de la configuración del sistema

Puede especificar la configuración del sistema que controla la forma en que vCloud Director interactúa con vSphere y vShield Manager.

El proceso de configuración crea una carpeta en vCenter para que la utilice vCloud Director y especifica el Id. que se debe utilizar al crear direcciones MAC para NICs virtuales.

Procedimiento

1 Especifique el nombre de la carpeta de vCloud Director vCenter en el campo **Nombre del sistema**.

2 Utilice el campo **Id. de instalación** para especificar el Id. de esta instalación de vCloud Director.

   Si el centro de datos incluye varias instalaciones de vCloud Director, cada instalación debe especificar un Id. de instalación único.

Listo para iniciar sesión en vCloud Director

Después de proporcionar toda la información que requiera el asistente para la configuración, puede confirmar los ajustes configurados y finalizar el asistente. Una vez que finalice el asistente, se abre la pantalla de inicio de sesión de la consola web de vCloud Director.

La página Listo para iniciar sesión enumera todos los ajustes de configuración que ha proporcionado al asistente. Examínelos detenidamente.

Prerequisitos

Verifique que tenga acceso a vCenter y a vShield Manager. La consola web de vCloud Director requiere el acceso a las instalaciones de vCenter y vShield Manager que desee configurar como parte de esta instancia de vCloud Director. Dichas instalaciones deben estar en ejecución y se deben haber configurado de modo que puedan trabajar una con la otra antes de que finalice esta tarea. Si desea más información, véase "Requisitos de hardware y software de vCloud Director," página 9.

Procedimiento

- Para cambiar algún valor, haga clic en **Atrás** hasta que llegue a la página donde se haya originado el valor.
- Para confirmar todos los ajustes de configuración y completar el proceso de configuración, haga clic en **Finalizar**.

Al hacer clic en **Finalizar**, el asistente aplica la configuración que haya especificado y luego inicia la consola web de vCloud Director y muestra la pantalla de inicio de sesión.

Qué hacer a continuación

Inicie sesión en la consola web de vCloud Director con el nombre de usuario y la contraseña que proporcionó para la cuenta del administrador del sistema. Después de iniciar sesión, la consola muestra un conjunto de pasos de inicio rápido que debe completar antes de utilizar la nube. Una vez que finalice los pasos, se habilitan las Tareas guiadas y la nube está lista para utilizarse.

Índice